TWO CONFLICTING APPROACHES TO § 512(C): *IO V. VEOH* AND *UMG V. VEOH*

Kuruvilla J. Olasa

Nicknamed Web 2.0,[1] today's Internet has democratized the creation and distribution of content.[2] Blogs, wikis, video sharing websites, and social networking sites allow individuals to reach a global audience at a relatively low cost and without any special technical knowledge.[3] This possibility of cheap, broad distribution has led to an explosion in content submitted by individuals and end users, dubbed user-generated content (UGC).[4] UGC covers a broad spectrum: software,[5] original digital videos,[6] news and commentary,[7] and even pornography.[8]

The rise of UGC threatens the traditional content creation industry in at least two ways. The first threat is through increased competition, which occurs because these new sources of content now vie for consumer attention. This competitive threat can prove socially useful because it gives users more choices and may force the traditional content industry to innovate.[9] Unfortunately, the same platforms that make UGC possible also threaten the content industry in a less socially useful way—through rampant copyright infringement. Some users take advantage of the distribution services that UGC platforms make possible to illicitly distribute copyrighted content to a wide audience.

Understandably threatened, and unwilling or unable to go after every end user, the content industry has instead targeted the service providers that host

---

1. Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY, Sept. 30, 2005, http://oreilly.com/web2/archive/what-is-web-20.html.

2. *See* Lisa Lapan, *Network Television and the Digital Threat*, 16 UCLA ENT. L. REV. 343, 348–54 (2009).

3. *See id.*

4. *See* Michael S. Sawyer, *Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA*, 24 BERKELEY TECH. L.J. 363, 367–68 (2009).

5. For example, Kongregate, located at http://www.kongregate.com/ is a UGC website dedicated to computer games.

6. For example, YouTube.com.

7. For example, CNN.com's iReport.

8. For example, YouPorn.com.

9. *See* Lisa Lapan, *supra* note 2, at 370.

these UGC platforms.[10] Given the scale of alleged infringement and the large damages available under the Copyright Act, these lawsuits against service providers threaten to put them entirely out of business.[11] Fortunately for service providers, copyright law grants them a powerful tool that could potentially protect their business models and shield them from liability—§ 512 of the Digital Millennium Copyright Act (DMCA) and its four safe harbors.[12]

Enacted in 1998, the DMCA gives qualifying service providers access to a number of safe harbors that dramatically limit their liability.[13] However, determining whether a service provider qualifies for a safe harbor has been a difficult question that has recently troubled courts and commentators.[14] Although the DMCA was enacted over a decade ago, the measured pace of judicial process has meant that much of the statute is only now being interpreted by the courts.

One requirement to qualify for two of the safe harbors, §§ 512(c) and (d), is that the service provider must not directly benefit from infringing activity if it also has the right and ability to control the infringing activity.[15] For service providers that do benefit from infringing activity on their systems, the safe harbor could turn on a single question: when does a service provider have the right and ability to control infringing activity? Two recent cases address this issue.

In *Io Group, Inc. v. Veoh Networks, Inc.*[16] and *UMG Recordings, Inc. v. Veoh Networks Inc.*,[17] two different plaintiffs sued the same online video provider

10. *See* Metro-Golden-Mayer Studios, Inc. v. Grokster, LTD, 545 U.S. 913, 929–30 (2005) ("When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability . . . ."); *see, e.g.*, Complaint at 2–3, Viacom Int'l, Inc. v. YouTube, Inc. No. 07 CV 2103 (S.D.N.Y. Mar. 13, 2007).

11. *See* 17 U.S.C. § 504(c) (2006) (establishing significant statutory damages for each act of infringement).

12. *See* 17 U.S.C. § 512(a)–(d) (2006).

13. 17 U.S.C. § 512(a)–(d).

14. *See, e.g.*, Ellison v. Robertson, 357 F.3d 1072, 1081 (9th Cir. 2004); ALS Scan, Inc. v. RemarQ Cmtys, Inc., 239 F.3d 619, 623–25 (4th Cir. 2001); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1099–1110 (W.D. Wash. 2004); Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1088–94 (C.D. Cal 2001); Mark A. Lemley, *Digital Rights Management: Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 113–14 (2007).

15. 17 U.S.C. § 512(c)(1)(B) (stating that to qualify for safe harbor a service provider must "not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity"); 17 U.S.C. § 512(d)(2) (same).

16. 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

17. 665 F. Supp. 2d 1099 (C.D. Cal. 2009).

for copyright infringement. In both cases the defendant, Veoh Networks, won summary judgment under the theory that it was entitled to a safe harbor under § 512(c) of the DMCA.[18]

Although the *Io* and *UMG* courts both found that Veoh did not have the right and ability to control infringing activity, the opinions reveal that both courts had different, incompatible understandings of § 512(c). The Note explains that the *Io* court's view of § 512(c) focused on the *practical* ability of a service provider to control infringement, holding that § 512(c) does not shield against vicarious liability claims. In contrast, the *UMG* court did not consider a service provider's practical ability to control infringement, holding that § 512(c) can shield a service provider against vicarious infringement claims. Finally, the Note argues that the *UMG* court better interprets § 512(c).

I. THE DMCA AND § 512(C) SAFE HARBOR

A. THE DMCA

The DMCA, enacted in 1998, is the most significant amendment to the Copyright Act of 1976.[19] According to its legislative history, the DMCA was "designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[20]

Title I of the DMCA implements two treaties of the World Intellectual Property Organization, to which the United States is a party.[21] One of its provisions, known as the "anti-circumvention" provision, effectively outlaws the circumvention of technical measures used to safeguard a copyrighted work.[22] For example, this provision outlaws removing the digital rights management (DRM) used to protect a downloadable movie. The DMCA's legislative history indicates that Title I was intended to encourage content providers to make their content available electronically.[23] By providing copyright owners enhanced copyright protection, such as the anti-circumvention provision, the legislation tried to give owners "reasonable assurance that they will be protected against massive piracy."[24] It was thought that this assurance would "facilitate making available quickly and

18. *Io*, 586 F. Supp. 2d at 1154–55; *UMG*, 665 F. Supp. 2d at 1118.

19. *See* David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 912 (2002).

20. S. REP. NO. 105-190, at 1–2 (1998).

21. *Id.* at 2.

22. *See* 17 U.S.C. § 1201 (2006).

23. S. REP. NO. 105-190, *supra* note 20, at 8.

24. *Id.*

conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius."[25] Initially, this part of the DMCA attracted the most attention and concern from commentators.[26] However, more recently, Title II has begun to emerge from the shadow of Title I.[27]

While Title I was intended to address the concerns of the content industry, Title II was aimed at allaying the concerns of internet service providers (ISPs).[28] Congress recognized that courts had already begun to apply common law principles of liability to the online setting. Instead of abrogating these common law doctrines in favor of a statutory scheme, Congress decided to create certain safe harbors, islands of protection from the common law.[29]

Title II provides four safe harbors to online service providers that meet certain criteria.[30] Its purpose is to provide "certainty for copyright owners and Internet service providers with respect to copyright infringement liability online."[31] The explosion of internet services has made Title II's safe harbors play a significant role in the often contentious battle between content producers and content distributors.[32]

B. SECTION 512(C) SAFE HARBOR AND "THE RIGHT AND ABILITY TO CONTROL" CLAUSE

Section 512(c) safe harbor is one of the four safe harbors made available by Title II of the DMCA.[33] It shields a service provider from most liability for information residing on their systems or networks at the direction of a user.[34] Section 512(c) is probably the most important of the safe harbors for

25. *Id.*

26. *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH L.J. 519 (1999).

27. *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L & ARTS 233, 233–34 (2009).

28. S. REP. NO. 105-190, *supra* note 20, at 8.

29. *Id.* at 19 ("Rather than embarking upon a wholesale clarification of [secondary copyright liability] doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers.").

30. *See* 17 U.S.C. § 512 (2006).

31. S. REP. NO. 105-190, *supra* note 20, at 2.

32. *See, e.g.*, Complaint at 3–5, Viacom Int'l, Inc. v. YouTube, Inc., No. 07 CV 2103 (S.D.N.Y. Mar. 13, 2007).

33. The DMCA's four safe harbors cover (1) transitory network communications (2) system caching (3) information residing on systems or networks at the direction of a user and (4) information location tools. 17 U.S.C. § 512.

34. *See id.*

user-generated content sites because the entire business model of these sites often relies on hosting user content.

The statute specifies a number of requirements a service provider must meet in order to benefit from § 512(c)'s safe harbor.[35] One of these requirements is that a service provider must not financially benefit from the infringing activity at issue while simultaneously possessing the right and ability to control the infringing activity.[36] For a number of reasons discussed in this Part, the meaning of this clause has been in dispute. Specifically, courts and commentators disagree on what it means for a service provider to have the "right and ability to control infringing activity." The crux of the dispute is whether courts should independently interpret "right and ability to control" in the context of the DMCA or whether this clause actually codifies the doctrine of vicarious copyright infringement.

1. The Vicarious Infringement View

The dispute over the correct meaning of § 512(c)'s right and ability clause begins with its language. The language of § 512(c)(1)(B) resembles the language used to describe vicarious liability. Section 512(c) covers only service providers that "do[] 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."[37] Similarly, a defendant infringes vicariously where it "profits directly from the infringement and has a right and ability to supervise the direct infringer."[38] This closeness in language has led some people to assume that § 512(c)(1)(B) codifies the elements of vicarious liability.[39] To these commentators, "the right and ability to control"

35. To qualify for safe harbor under § 512(c), an entity must meet several requirements common to all safe harbors as well as a number of requirements specific to § 512(c). First, the entity must qualify as a service provider. § 512(k). Second, it must adopt and inform an account holder's policy that terminates "repeat infringers." § 512(i)(1)(A). Third, it must accommodate and not interfere with "standard technical measures." § 512(i)(1)(B). Fourth, it must not have actual knowledge of infringement and must not be "aware of facts or circumstances from which infringing activity is apparent," or if it does have such awareness it must act expeditiously to remove the infringing material. § 512(c)(1)(A). Fifth, it must "not receive a financial benefit directly attributable to the infringing activity, in a case in which [it] has the right and ability to control such activity." § 512(c)(1)(B). Sixth, it must implement a notice and takedown procedure. *See* § 512(c)(1)(C).

36. § 512(c)(1)(B).

37. *Id.*

38. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 931 n.9 (2005).

39. *See, e.g.*, CoStar Group, Inc. v. LoopNet, Inc., 164 F. Supp. 2d 688, 704–705 (D. Md. 2001) (holding that the DMCA codified common law), *rev'd.* 373 F.3d 544, 554 (4th Cir. 2004) (reversing this point on the codification of common law). *See also* Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1150–51 (N.D. Cal. 2008); Mark A. Lemley,

under § 512(c) is the same as "the right and ability to supervise" under vicarious liability.

One implication of the view that § 512(c)(1)(B) codifies vicarious liability is that vicarious liability claims are effectively excluded from the ambit of § 512(c).[40] In other words, under this view, § 512(c) does not shield service providers from vicarious infringement claims. Though the *Io* court adopted such an interpretation, the Note argues that this position is incorrect. But to understand why, it is first necessary to examine the doctrine of vicarious liability.

The Copyright Act does not directly provide for any form of secondary liability.[41] Instead, theories of secondary copyright liability are judge-created doctrines.[42] Vicarious liability, in particular, was developed "as an outgrowth of the agency principles of respondeat superior."[43] As Professor David Nimmer notes, vicarious liability traditionally arose in the "context of landlords of premises where infringement takes place."[44]

The Supreme Court addressed secondary liability and vicarious liability in the landmark cases of *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*[45] and *Sony Corp. v. Universal City Studios, Inc.*[46] But in both of these cases, the Court did not have an opportunity to examine the meaning of right and ability to control because it based its decisions on different doctrinal principles. However, the Ninth Circuit—dubbed "the court of appeals for the Hollywood circuit"[47] by Judge Kozinski—has had the opportunity to address this doctrine a number of times. Because the doctrine of vicarious copyright infringement is well-developed in the Ninth Circuit, and because the Note focuses on the conflict between two cases arising within the Ninth Circuit's jurisdiction, this discussion considers Ninth Circuit case law.

Under Ninth Circuit precedent, a service provider's right and ability to control an infringing activity appears to depend on three factors. First, a provider's right and ability to control is linked to the boundaries of its

Digital Rights Management: Rationalizing Internet Safe Harbors, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 113–14 (2007).

40. Lemley, *supra* note 39.

41. *Grokster*, 545 U.S. at 930 ("[T]he Copyright Act does not expressly render anyone liable for infringement committed by another." (quoting Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 434 (1984))).

42. *Id.*

43. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261–62 (9th Cir. 1996).

44. 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A][2] (2008).

45. 545 U.S. 913, 929–35 (2005).

46. 464 U.S. at 417.

47. White v. Samsung Elecs. America, Inc., 989 F.2d 1512, 1521 (Kozinski, J., dissenting).

premises. The provider is not responsible for infringement outside its premises but is responsible for policing its premises to the fullest extent. Second, the provider must be able to actually stop the infringing activity and not just deter it. It is not enough for the provider to make the infringement financially unattractive or more difficult. Finally, the capacity to stop infringement must be *practical*. The theoretical possibility of stopping infringement is not enough.

Fonovisa, Inc. v. Cherry Auction, Inc.[48] and *A&M Records, Inc, v. Napster, Inc.*[49] demonstrate that a service provider's premises define its right and ability to control infringing activity. In *Fonovisa*, the Ninth Circuit considered the vicarious liability of a swap meet operator for copyright infringement conducted by vendors it rented to.[50] The defendant, Cherry Auction, operated a swap meet where it rented booth space to vendors for a daily rental fee.[51] As part of the agreement, Cherry Auction provided advertising and parking, and it also retained the right to terminate vendors for any reason.[52] The court found that Cherry Auction's ability to exclude vendors was sufficient to give it the right and ability to control infringing activity.[53]

Napster applied *Fonovisa*'s principle to the online context. In *Napster*, the defendant's systems acted as a matchmaking service, connecting users searching for a file with users advertising that they had the file.[54] The defendant's system did not interact with the files themselves, nor did it transfer the files between users. Instead, the defendant possessed a database of file names that were matched up against the internet addresses of users who had the file.[55] The Ninth Circuit panel in *Napster* applied *Fonovisa* in a two-step process. First, it defined the extent of Napster's premises—the area it controlled.[56] Second, the court asked whether *Napster* policed its premises "to the fullest extent," as required by *Fonovisa*.[57]

To the first question, the court held that Napster's premises, the area it had a right and ability to control, were cabined by its system's architecture.[58] Napster had no ability to control or monitor the files or activity on its users' systems, but it did have the ability to monitor and control the central index it

48. 76 F.3d at 262–63.
49. 239 F.3d 1004, 1023–24 (9th Cir. 2001).
50. 76 F.3d at 261.
51. *Id.*
52. *Id.* at 261–62.
53. *Id.* at 262–63.
54. *See Napster*, 239 F. 3d at 1012–13.
55. *See id.*
56. *See id.* at 1023–24.
57. *Id.*
58. *Id.* at 1024 ("Napster's reserved 'right and ability' to police is cabined by the system's current architecture.").

maintained.[59] Therefore, the court defined Napster's premises to be its "file name indices."[60]

The court answered the second question, whether Napster fully exercised its control over its premises, in the negative.[61] According to the court, Napster had the ability to look through its search indices and, based on file name, remove those file names that corresponded to infringing content.[62] In this way, end users would not be able to locate these files. By failing to remove the names of infringing files from its network the defendant had failed to fully police its premises, and, by implication, had failed to exercise its right and ability to control the infringement.

Therefore, taken together, *Napster* and *Fonovisa* stand for a simple proposition: A service provider's right and ability to control infringing activity extends to the boundary of its properly defined premises. And in the online context, as the *Napster* court indicated, a service provider's right and ability to control is "cabined" by its system's architecture.

Next, a service provider does not have a right and ability to control infringing activity simply because it can control any activity related to the infringement. Instead, through its actions the service provider must be able to actually stop the infringement. In *Perfect 10, Inc. v. Amazon.com, Inc.*,[63] the court distinguished between an ability to discourage infringement and an ability to actually *control* it.[64] The copyright owner, Perfect 10, sued Google for linking to third party websites that contained infringing images and for marketing advertising space on these websites.[65] Google retained the power to terminate its contract with any website that committed copyright infringement, but allegedly did not exercise this power.[66] The court held that Google's power to terminate its business relationship with a website did not equate to the power to actually control infringement on that website: "An infringing third-party website can continue to reproduce, display, and distribute its infringing copies of Perfect 10 images after its [relationship with Google] has ended."[67] Similarly, in *Perfect 10, Inc. v. Visa International Service Association.*,[68] the court expanded on this distinction between the ability to deter and the ability to control. According to the court, "the mere ability to

59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*
63. 487 F.3d 701 (9th Cir. 2007).
64. *See id.* at 730.
65. *Id.* at 725–26.
66. *Id.* at 730.
67. *Id.*
68. 494 F.3d 788 (9th Cir. 2007).

withdraw a financial 'carrot' does not create the 'stick' of 'right and ability to control.'"[69]

Napster is consistent with this view. Although the actual infringement did not occur on the defendant's systems, the defendant still had the power to entirely stop the infringement through control of its system. By searching its indexes for copyrighted song names, Napster could effectively prevent its users from trading in those songs.

Finally, at least one Ninth Circuit panel has found that this ability to *control*, as opposed to discourage, infringement must also be practical.[70] The *Amazon* court held that in addition to a legal right to terminate infringing activity, a defendant had to have a "practical ability" to detect and terminate the activity.[71] The court held that the defendant, Google, lacked the right and ability to control infringement because it could not practically detect which images it linked to were infringing and which were non-infringing.[72] *Amazon*'s holding with respect to a practical ability to control is echoed in *Napster* as well. Like in *Amazon*, the *Napster* court focused on the defendant's actual ability to police its search indices.[73]

2. The Opposing View

Others reject the idea that the "right and ability" clause in § 512(c) is meant to reflect the common law meaning of vicarious liability, and that the statute cannot shield providers from vicarious liability claims. This camp points to the legislative history as well as the language of the DMCA to make their case.[74]

The legislative history contradicts the idea that § 512(c) excludes vicarious liability in two distinct ways. First, the legislative history states that Congress both recognized that courts had begun to apply vicarious liability to online service providers and wished to leave that law in its currently evolving state while carving out certain safe harbors.[75] Second, the record indicates

69. *Id.* at 803.

70. Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 730 (9th Cir. 2007).

71. *Id.* at 731.

72. *Id.*

73. *See* A&M Records, Inc, v. Napster, Inc., 239 F.3d 1004, 1024 (9th Cir. 2001).

74. *See* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001); Lee, *supra* note 27, at 237.

75. S. REP. NO. 105-190, *supra* note 20, at 19 ("Rather than embarking upon a wholesale clarification of [secondary copyright liability] doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers.").

that Congress believed the safe harbors would be used to shield service providers from vicarious liability.[76]

Furthermore, those who oppose the "vicarious liability view" point out that interpreting the benefit and control exclusion as a codification of vicarious liability would render the statute internally inconsistent.[77] The inconsistency arises because the DMCA presumes that service providers already have the right and ability to control their systems. In the view of these commentators, it would be illogical for the DMCA to deny service providers access to the safe harbor because of something the DMCA itself requires them to be able to do. Therefore, these commentators argue that the "right and ability to control" language in the statute should be interpreted as a departure from the meaning of that phrase in the vicarious liability context.[78]

II. *IO GROUP* & *UMG*'S SAFE HARBOR ANALYSIS

A. BACKGROUND ON VEOH NETWORKS

Veoh Networks is a video service provider that allows users to upload their own videos and share them with others. Since its inception, hundreds of thousands of users have uploaded and shared videos on Veoh's systems.[79] To upload a video to Veoh's systems, a user must first create an account.[80] After the account is created, the user can upload video in a variety of file formats.[81] As part of this upload process, Veoh automatically converts the video into the "Flash" format and extracts several still images from the file.[82] Veoh occasionally spot checks videos to ensure that they comply with its terms of use.[83]

Veoh has published a "Terms of Use" as well as an "Acceptable Use Policy."[84] These documents inform users that Veoh reserves the right to block content or terminate users for violations of Veoh's policies, including

76. *See id.* at 40 ("The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement.").

77. *Hendrickson*, 165 F. Supp.2d at 1093–94.

78. *See id.*; Lee, *supra* note 27, at 237.

79. Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1136 (N.D. Cal. 2008).

80. *Id.*

81. *Id.*

82. *Id.* at 1138–40.

83. *Id.* at 1140.

84. *Id.* at 1137–38.

the unauthorized posting of copyrighted material.[85] Nevertheless, many users upload infringing content onto Veoh's servers.[86]

B. *IO GROUP V. VEOH NETWORKS*

In *Io Group v. Veoh Networks*, Io Group, an adult content creator, sued Veoh for copyright infringement.[87] According to Io, Veoh was liable for infringement because it allowed users to upload and share Io's copyrighted content.[88] Specifically, Io claimed to have discovered that clips from ten of its films had been uploaded and viewed on Veoh without authorization.[89] Io moved for summary judgment on the issue of liability, and Veoh cross-moved for summary judgment on the applicability of the § 512(c) safe harbor.[90] The court first addressed Veoh's motion and held that Veoh was shielded from liability under § 512(c).[91] As a result, the court found that Io's motion was moot because the relief it sought was precluded by the safe harbor.[92]

In its opinion, the *Io* court methodically determined that Veoh met every requirement of the § 512(c) safe harbor. One of these requirements is § 512(c)(1)(B), which excludes a service provider from the safe harbor if it receives a direct financial benefit from the infringing activity while having the right and ability to control the activity.[93] After adopting a form of the "vicarious liability" view of § 512(c), the court ruled that Veoh did not have a right and ability to control infringement because it lacked the practical ability to limit infringing activity.[94]

The court started its analysis by holding that § 512(c)(1)(B)'s "right and ability to control" clause codifies the similar language from vicarious copyright liability.[95] Essentially, the court adopted the "vicarious liability" view discussed in Part II. The court did not provide a reason for this holding, except to note that in *Perfect 10, Inc. v. CCBill LLC*,[96] the Ninth Circuit had held that § 512(c)'s "financial benefit" clause should be interpreted consistent with the similar language from vicarious infringement. Thus, it appears that

85. *Id.* at 1138.
86. *Id.* at 1136.
87. *Id.* at 1135.
88. *Id.* at 1136–37.
89. *Id.*
90. *Id.* at 1135.
91. *Id.* at 1154–55.
92. *Id.*
93. *See supra* Part II.B.
94. *Io*, 586 F. Supp. 2d at 1153–55.
95. *Id.* at 1150.
96. *Id.* (citing Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007)).

the *Io* opinion implicitly accepts that the Ninth Circuit's reasoning regarding "financial benefit" should be applied to "right and ability to control" as well.

After the court adopted the vicarious liability view, it was able to make use of vicarious liability case law in order to assess whether Veoh had the right and ability to control infringing activity on its system.[97] According to the court, "a defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so."[98]

Looking at the specific facts in the case before it, the court found that Veoh did not have the right and ability to control infringing activities on its system because it lacked the practical ability to identify and remove infringing videos. As the court noted, "no reasonable juror could conclude that a comprehensive review of every file [uploaded to Veoh] would be feasible."[99] And, according to the court, "Veoh's ability to control its index does not equate to ability to identify and terminate *infringing* videos."[100] Simply put, in the view of the *Io* court, although Veoh had the legal right to block infringing videos and the technological ability to do so as well, it lacked the necessary "practical" ability to both identify and block such videos.

An important implication of the *Io* court's approach to the § 512(c) safe harbor is the way it ties system design and capability to eligibility for the safe harbor. This implication is a consequence of importing the "practical" ability to control standard from vicarious liability into safe harbor design. As the court noted: "At least one court has observed that the requisite 'right and ability to control' 'presupposes some antecedent ability to limit or filter copyrighted material.'"[101] Veoh did not have the practical ability to control infringement because its system did not give it such an antecedent ability.[102] In contrast, according to the court, Napster's system did have such an antecedent ability, and therefore was found to have the requisite right and ability to control.[103]

The strongest support for the idea that under *Io*, system design and right and ability to control are strongly intertwined is explicitly found in the court's own language: "Perhaps most importantly, there is no indication that Veoh has failed to police its system to the fullest extent permitted by its

97. *See* Part II.

98. *Io*, 586 F. Supp. 2d at 1150 (citing Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007)).

99. *Id.* at 1153.

100. *Id.*

101. *Id.* at 1151 (quoting Tur v. YouTube, Inc., No. CV064436, 2007 U.S. Dist. LEXIS 50254, 2007 WL 1893635 at *3 (C.D. Cal., June 20, 2007)).

102. *Id.* at 1153.

103. *Id.*

architecture."[104] Therefore, Veoh's ability to control its network is closely informed by its system design.

As the next section shows, the *UMG* court took a drastically different approach to interpreting right and ability—an approach in which a service provider's "right and ability to control" infringing activity is significantly less dependent on system design.

C. *UMG RECORDINGS V. VEOH NETWORKS*

Universal Music Group (UMG), a record company, sued Veoh for reasons similar to those in *Io*.[105] *UMG* claimed that Veoh was liable for infringement because it stored and disseminated audiovisual works owned by UMG. As in *Io*, Veoh moved for summary judgment that it was entitled to § 512(c)'s safe harbor.

Although the issues in *UMG* and *Io* are extremely similar, there was at least one important factual difference. In *UMG*, the plaintiff claimed that the defendant took too long to implement a filtering system known as "Audible Magic."[106] Audible Magic is a third party product that is designed to filter out copyrighted content. It works by taking a "fingerprint" of each video and comparing it to a database of copyrighted work.[107] Veoh began to use Audible Magic to screen files as users uploaded them, but UMG complained that Veoh should have adopted the technology sooner.[108] UMG also argued that Veoh should have run Audible Magic on its "back catalog"—works that had been uploaded before Audible Magic was used.[109]

The *UMG* court recognized that the DMCA's text constrained the court's interpretation of "right and ability to control" in two ways. One constraint was that the DMCA already presupposes that a service provider can control its own network.[110] The second constraint, and the one that separated *UMG*'s analysis from *Io*'s, was § 512(m), which states that the applicability of the four safe harbors should not be conditioned on a service provider taking any affirmative steps to police its network.[111]

UMG's initial analysis is congruent with *Io*'s. As in *Io,* the *UMG* court recognized that it is untenable to read "right and ability to control" to mean

104. *Id.*

105. UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1100 (C.D. Cal. 2009).

106. *Id.* at 1111.

107. *Id.* at 1103.

108. *Id.* at 1111.

109. *Id.* at 1102 n.5.

110. *Id.* at 1115.

111. *See id.*

no more than the service provider's ability to control its own network.[112] Multiple sections of § 512(c) presuppose that all service providers have this ability.[113] As the court recognized, "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA."[114]

UMG parts ways with *Io* when it recognizes an additional constraint in interpreting the statute. Section 512(m) provides: "[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 . . . ."[115] According to the court, any interpretation of § 512(c) would need to be consistent with § 512(m) as well. Therefore, § 512(c)'s applicability could not be conditioned on requiring a service provider to affirmatively police its network.[116]

The additional constraint imposed by § 512(m) effectively precludes holding that right and ability to control retains its common law meaning because the common law standard for vicarious liability conditions liability on whether a provider has fully policed its system and excluded infringing users. For example, in *Napster*, the defendant was liable because it failed to fully police its file indexes.[117] Interpreting "right and ability to control" to be a codification of one of the elements of vicarious liability, as the *Io* court did, would contravene the clear meaning of § 512(m) and render the statute inconsistent.

Therefore, the *UMG* court recognized that: (1) right and ability to control could not mean the mere ability to exclude users, but (2) neither could it mean the same as vicarious liability's "right and ability to control" requirement.[118] As a result, the court was forced to apply its own statutory analysis.[119]

To resolve this tension, the court employed a different approach from the approach in *Io*. Instead of trying to *qualitatively* distinguish control of a system from control of an activity, the *UMG* court found that the level of control required to trigger the exclusion was simply *quantitatively* more than

112. *Id.* at 1113.

113. *Id.* at 1112.

114. *Id.* at 1113 (quoting Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1093–94 (C.D. Cal 2001)).

115. 17 U.S.C. § 512(m) (2006).

116. *UMG*, 665 F. Supp. 2d at 1113.

117. *See supra* Part II.B.

118. *See UMG*, 665 F. Supp. 2d at 1115.

119. *Id.*

mere ability to control ones system.[120] In the court's view, the right and ability to control infringement has less to do with the service provider policing their own system, and more to do with the level of control exerted in the content distribution process.[121] The court looked to two cases to determine the level of control necessary to trigger the exclusion.

In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,[122] the court found that a defendant had the "right and ability to control" infringement with regards to § 512 when it prescreened websites, gave them extensive advice, and prohibited the proliferation of other identical websites.[123] Similarly, the court pointed to *Corbis Corp. v. Amazon.com, Inc.*, which held that a defendant did not have a right and ability to control infringement under § 512 because it did not involve itself in any way with transactions on its website.[124] Thus, although the court did not explicitly say so, it is possible that the key distinction lies between service providers that passively accept content, and those that partake in some kind of an active editorial role.

III. COMPETING APPROACHES TO § 512(C)

Because *Io* and *UMG* came to the same conclusion regarding Veoh's right and ability to control infringement, one might at first glance view the decisions as interchangeable. But such a conclusion would miss key distinctions between the courts' reasoning. Although both cases reached the same result, they employed fundamentally different approaches that could have important implications going forward.

First, the *Io* reasoning would permanently link § 512(c) with common law vicarious liability; both would necessarily evolve together under this view. In contrast, the *UMG* view would ensure that interpretation of § 512(c) will not restrict the broader evolution of vicarious liability. Second, the standard established in *Io* would require courts to closely consider the design and practical limitations of a service provider's system in order to determine the extent of its right and ability to control. Finally, under the *Io* view, a service provider's ability to control infringement might encompass affirmative policing of its network. *UMG* instead provides a simpler conduct-based rule. Perhaps the clearest way to see the incompatibility between the two approaches is to apply *Io*'s reasoning to the slightly different facts in *UMG*.

120. *See id.*
121. *See id.*
122. 213 F. Supp. 2d 1146 (C.D. Cal. 2002).
123. *See UMG*, 665 F. Supp. 2d at 1114 (citing *Cybernet*, 213 F. Supp. 2d at 1181–82).
124. *See id.* (citing Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004)).

A. UNIFICATION

Io's approach unifies the right and ability clause in vicarious liability with the right and ability clause under § 512(c). This unification could have one of two effects: It could either restrict the evolution of the vicarious liability doctrine in a way consistent with the DMCA, or it could create internal inconsistencies within the DMCA. By contrast, *UMG*'s approach allows vicarious liability and § 512(c) to develop independently, but risks undermining the coherence of copyright law.

Io's approach links the interpretation of § 512(c)'s right and ability clause to the continually evolving doctrine of vicarious copyright liability. Under this approach, when a court needs to decide whether a service provider has the right and ability to control infringement, the court can and should look to precedent that applies the clause in either the safe harbor context or the vicarious liability context. Vice-versa, a court considering an issue of vicarious liability must consider decisions in both contexts as well. The essential point is this: now that they are linked, the vicarious liability "right and ability" clause and the § 512(c) "right and ability" clause must evolve in lockstep. Decisions interpreting the clause in any context affect both versions of the clause.

This lockstep evolution affects the development of the vicarious liability doctrine in a crucial way—it requires the doctrine to evolve in a way consistent with the DMCA. A court decision interpreting "right and ability" in a non-service provider context will still need to consider the DMCA. This is because when the court interprets the clause that interpretation will now also control in cases that are subject to the DMCA. In effect, the language of the DMCA will constrain the development of the common law doctrine of vicarious liability.

One example of such a constraint is § 512(m). This section of the DMCA states that a service provider's liability cannot be conditioned on any affirmative steps it takes to police infringement.[125] Any interpretation of "right and ability to control" in the DMCA context must conform to this restriction. But now, in addition, a court interpreting "right and ability" in an ordinary landlord-tenant context must adhere to this restriction as well and not impose any affirmative duties on landlords. If the court does impose affirmative duties it risks introducing an inconsistency into the DMCA.

UMG's approach sidesteps this problem, but in a potentially messy way. Under *UMG*, vicarious liability is free to develop on its own, without additional statutory restrictions. Separate inquiries as to a service provider's "right and ability to control" infringement are made in the liability context

125. *See* 17 U.S.C. § 512(m) (2006).

and in the safe harbor context. Furthermore, a decision of a court in the safe harbor context need not affect the analysis of a court in the liability context.

However, *UMG*'s approach is messy—it undermines the possibility of a coherent copyright doctrine. Terms such as "direct financial benefit" and "right and ability to control" have traditionally held single, if constantly evolving, meanings. *UMG*'s approach destroys the possibility of such terms to have universally understood meanings. However, by explicitly creating affirmative safe harbors, the DMCA may, arguably, have intended to fragment copyright law.

B. DIFFERENT STANDARDS

A second, more fundamental, difference between *Io* and *UMG* is found in the standard each court developed. *Io*'s standard focuses on the practical ability of a service provider to stop infringement, an approach that requires the court to closely consider overall system design. And *Io*'s approach may also require a service provider to take affirmative steps in exercising this practical ability to control infringement. On the other hand, *UMG*'s approach requires the court to consider conduct and does allow for any affirmative duties on a service provider's part.

The *Io* decision focuses on "practical" limitations. As discussed in Part II, Veoh was held not to have the right and ability to control infringement because it simply was not capable of detecting infringing videos from the hundreds of thousands of videos it received. The court's analysis therefore proceeds as follows: (1) what are the overall capabilities of the defendant's system, including technical capabilities and business capabilities, and (2) given these capabilities was it practical for the defendant to detect and block infringement.

Determining the contours of a defendant's capabilities can be a highly technical task. For example, things like the efficacy of filters, the usefulness of spot-checks, and the usefulness of user-flagging systems can all be very empirical questions. Analyzing the issue of filters alone may require both sides to present expensive technical reports.

The second step is equally problematic. Given the defendant's capabilities, the court must determine whether it was "practical" for the defendant to block infringement. It is unclear what this means, but arguably the court could apply a tort-like "reasonableness standard" and assess the costs of policing the network against the potential benefits. One of the possible effects of this rule is that it allows ISPs with fewer capabilities to have less of a duty to police their networks. As such, it creates an incentive for ISP's to act strategically and not implement or design ways to reduce copyright infringement.

In contrast, the *UMG* approach does not consider the practical capabilities of the service provider in determining the applicability of § 512(c). Instead the court looks to the level of involvement between the service provider and the infringing activity.

C. THE *IO* AND *UMG* APPROACHES CANNOT BE RECONCILED

More than just representing different approaches to interpreting benefit and control, the *Io* and *UMG* decisions are fundamentally incompatible with each other. The clearest way to see this incompatibility is by applying the *Io* court's analysis to the facts from *UMG*. If the *UMG* court had adopted *Io*'s analytical framework, the case's outcome would likely have been completely different.

One of the major reasons the *Io* court found that Veoh was not excluded from the safe harbor was because there was no indication that Veoh did not police its network to the fullest extent possible.[126] To the *Io* court, determining whether Veoh policed its network to the fullest extent possible was a matter of practicalities: Veoh did not have the practical ability to comb through hundreds of thousands of videos.[127] Therefore, the court determined that there was no right and ability to control infringement.[128] In the view of the court, Veoh's ability to police its network was "cabined" by its architecture.

In *UMG*, the facts were subtly different. In that case there was evidence that Veoh had an automated filter to process and identify copyrighted content.[129] Veoh used the filter to identify copyrighted works being uploaded, but failed to apply the filter to its back-catalog of works already on the system.[130] Arguably, Veoh had not policed its system to its fullest extent—its ability to do so was no longer constrained by its architecture. In fact, its new architecture made it possible for it to employ at least limited policing.[131] Therefore, under the *Io* court's analysis, Veoh most likely would not be entitled to safe harbor because it was capable of policing its premises.

In contrast, the *UMG* court viewed the Audible Magic system as an affirmative effort on the part of Veoh, one that it was not required to undertake.[132] Although such affirmative efforts do not lead to additional

126. Io Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1153 (N.D. Cal. 2008).

127. *Id.*

128. *Id.*

129. UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1103 (C.D. Cal. 2009).

130. *Id.*

131. *Id.*

132. *Id.* at 1113.

liability under *UMG*'s analysis, they might under *Io*'s. This is because under *Io*, a service provider like Veoh could alter the current architecture of the system and thereby alter the extent of policing required.

IV. *UMG*, *IO*, AND STATUTORY INTERPRETATION.

Two strands of statutory interpretation support *UMG*'s interpretation of § 512(c) over *Io*'s. First, § 512's text supports *UMG*'s view that § 512(c) does not codify the doctrine of vicarious liability. Second, the legislative history of § 512 supports UMG's view.

A. SECTION 512'S TEXT

Statutory text is generally the best starting point in interpreting a statute.[133] In the case of § 512(c)'s benefit and control clause, the statutory text is extremely ambiguous. This is entirely unsurprising because if the text of § 512(c) were clear, courts would have little trouble interpreting it. In fact, the text provides strong support for both the *Io* interpretation of § 512(c) as well as the *UMG* interpretation.

The *Io* view finds support in the similarity of language between § 512(c) and the way many courts have described vicarious liability. When interpreting a statute, any "special senses" a particular word or phrase has acquired should be considered.[134] Therefore, it seems reasonable that § 512(c) should be interpreted consistent with the "special sense" of vicarious liability its language seems to convey. But there are two problems with this argument. First, although the language is similar, it is not exact. As Professor Edward Lee notes, no court has ever used § 512(c)'s exact language to describe vicarious liability.[135] This undercuts the idea that the exact language used in the statute has any special meaning. But more importantly, if Congress did want to encapsulate vicarious liability into section § 512(c), a much simpler label existed: the term "vicarious liability" itself. If § 512(c) was intended to incorporate the special meaning of a common law principle then it could have done so by either using the exact language of the doctrine or, more simply, the well-understood name of the doctrine.

Additionally, the existence of § 512(m) undercuts the *Io* view and supports the *UMG* view. A statutory provision's meaning can be illuminated by considering a separate section of the statute. Here, § 512(m) sheds light on the meaning of § 512(c)'s benefit and control clause. According to § 512(m), the applicability of the safe harbors should not be conditioned on a service

133. *See* William N. Eskridge, Jr. & Philip P. Frickey, *Statutory Interpretation as Practical Reasoning*, 42 STAN. L. REV. 321, 354 (1990).

134. *Id.*

135. *See* Lee, *supra* note 27, at 240.

affirmatively monitoring its service.[136] *Io*'s view of the statute does not take § 512(m) into account. In fact, under *Io*'s view a service provider does have a duty to police its network where feasible. In contrast, *UMG*'s view does not require a service provider to take any affirmative acts.

Therefore, the statutory text is ambiguous at best. While there is support for the idea that § 512(c)'s language has a "special sense," the support is not unequivocal. Furthermore, there is support for the argument that § 512(c) cannot encapsulate vicarious liability because of § 512(m). This ambiguity can be resolved by looking to the history and the purpose of the statute.

B. LEGISLATIVE HISTORY AND PURPOSE

The legislative history and purpose of the DMCA strongly support *UMG*'s view over *Io*'s view. In the legislative history of the DMCA, Congress explicitly mentions that instead of clarifying the common law doctrines of copyright liability, it instead decided to carve out four safe harbors.[137] The common law doctrines were to be left in their evolving state. This strongly supports the view that Congress wished to create statutory safe harbors that would protect a service provider under whatever common law regime of liability existed at the time. Interpreting § 512's right and ability to control to be a codification of vicarious liability would not further Congress's goal. Instead it would closely tie the common law standards to the statutory safe harbor, frustrating Congress's purpose.

Congress also intended that the DMCA provide service providers "certainty." The standards of liability at the time were direct infringement as well as the common law doctrines of secondary liability—doctrines that Congress seemed especially concerned about. If Congress viewed the existing regimes of liability as too uncertain for service providers, it would make no sense to then import these standards.

Furthermore, moving from the abstract to the practical, the *Io* approach provides significantly less certainty to service providers than *UMG*'s approach. As discussed, *supra*, in Part II, *Io*'s approach makes a service provider's liability depend on its system design, in contrast to *UMG*'s approach, which focuses more on the provider's editorial control. This makes *Io*'s approach significantly more uncertain because each provider's capabilities to police its system will need to be tested in court. In contrast, by focusing on a service provider's *extent* of involvement with infringement, a

136. *See* 17 U.S.C. § 512(m) (2006).

137. S. REP. NO. 105-190, *supra* note 20, at 19 ("Rather than embarking upon a wholesale clarification of [secondary copyright liability] doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors,' for certain common activities of service providers.").

provider can more easily limit its liability by just figuring out where courts have drawn the line.

For example, under the *Io* approach, the service provider's ability to filter or review every video is an important consideration. But this capability is likely to be constantly in flux as technology or available resources change. But under the *UMG* approach, the service provider's liability is more closely tied to its business model and level of involvement. Regardless of the underlying system, technology, or capabilities a protected business model will be protected for all service providers.

Finally, in at least one place the legislative history of the DMCA explicitly indicates that it is intended to apply to claims of vicarious liability.[138] This makes sense; vicarious liability claims are likely the most common claims a service provider will encounter. A safe harbor regime that does not cover such claims would be a half solution indeed. The presence of such clear language in § 512's legislative history provides ample support for *UMG*'s view.

V. CONCLUSION

Considering the high stakes, § 512 and its four safe harbors are likely to play an increasingly important role in conflicts between service providers and the content industry. Therefore, it is crucial that courts become familiar with interpreting and administering these safe harbors. Perhaps more importantly, to reduce legal costs and uncertainly, courts need to develop uniform, consistent interpretations of the complex provisions of these safe harbors.

The disagreement over how to interpret § 512(c)'s right and ability to control clause is just one, albeit important, conflict that must be resolved in order for courts to develop a uniform, consistent § 512 jurisprudence. The *Io* and *UMG* courts have provided us with two very different interpretations of § 512(c). In *Io,* the court found that § 512(c)'s right and ability clause codifies the common law doctrine of vicarious copyright infringement. This interpretation means that a service provider's right and ability to control infringement is closely tied to its practical ability to control infringement. Furthermore, under this view a service provider may be under an obligation to take affirmative steps to police its network. In contrast, the *UMG* court rejects the idea that § 512(c) codifies vicarious liability. Instead, for the *UMG* court, a service provider's "right and ability" to control is connected to its level of involvement with the infringing activity. Although both approaches

138. *Id.* at 40 ("The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement.").

find support in the text of § 512(c), the *UMG* approach appears to better reflect Congress's goal in creating the safe harbors.