SHOOTING THE MESSENGER: ISP LIABILITY FOR CONTRIBUTORY COPYRIGHT INFRINGEMENT

David Ludwig*

JUDICIAL ENFORCEMENT OF CONTRIBUTORY COPYRIGHT INFRINGEMENT CLAIMS AGAINST INTERNET SERVICE PROVIDERS AND JUDICIAL INTERPRETATION OF THE DMCA SAFE HARBOR PROVISIONS

I. Introduction
II. Contributory Copyright Infringement
   A. Knowledge Requirement
   B. Material Contribution Requirement
III. Digital Millennium Copyright Act Safe Harbor Provisions
   A. Threshold Requirements Under § 512(i)
   B. No Monitoring Required Under § 512(m)(1)
   C. Limitations on ISP Liability Under § 512(a)-(d)
   D. Judicial Enforcement of Contributory Copyright Infringement Claims Against ISPs
   E. Interpretation of Contributory Infringement
      i. The Slippery Knowledge Requirement: From Sony to Netcom and Grokster ...
      ii. Material Contribution as Given: Misreading Sony and Netcom
   F. Application of the DMCA Safe Harbor Provisions
      i. Misreading the Threshold Requirements
      ii. Willful Blindness and § 512(m)(1)
      iii. Shooting the Messenger: Why ISP Liability Is the Wrong Answer
IV. Conclusion

I. INTRODUCTION

Internet Service Providers (ISPs) [1] are an essential component of the internet: they enable users and content providers to connect with one another online. [2] In enacting the Digital Millennium Copyright Act (DMCA), the purpose of which was to strengthen copyright protections in the digital realm, Congress recognized both the important role played by ISPs and the danger of copyright infringement liability for ISPs under existing case law. In response to this concern, Congress included the Online Copyright Infringement Liability Limitation Act (OCILLA) safe harbor provisions [3] to shield innocent ISPs from liability for contributory copyright infringement.
Recent trends in judicial enforcement of contributory copyright infringement claims against ISPs and judicial interpretation of the DMCA safe harbor provisions, however, undermine the balance sought by Congress in the DMCA by imposing excessive liability upon ISPs. [4] The danger of this trend is that such enforcement will have a significant chilling effect on ISP investment in the internet, which fosters both the growth of e-commerce and the ability of a larger segment of the population to participate in the internet community-- both of which ultimately benefit the holders of intellectual property rights.

Shielding ISPs from liability for contributory copyright infringement in accord with the DMCA safe harbor provisions does not leave copyright holders without the means to prevent infringement in the digital realm. The DMCA offers numerous options for copyright holders in cyberspace that are not available in “real space,” such as the technological self-help anti-circumvention provisions of 17 U.S.C. § 1201, [5] the subpoena provisions of 17 U.S.C. § 512(h) [6] that enable copyright holders to locate and bring suit against direct infringers, and the notice and takedown provisions of 17 U.S.C. § 512(b)-(d). [7]

Parts II and III of this note discuss the law of contributory copyright infringement and the safe harbor provisions of the DMCA, respectively. Part IV discusses recent judicial enforcement of contributory copyright infringement claims against ISPs and the interpretation and application of the DMCA safe harbor provisions in those cases. Part V discusses the policy implications of such decisions and argues for a more faithful judicial adherence to the congressional mandate.

II. Contributory Copyright Infringement

There is no statutory basis for a claim of contributory copyright infringement, [8] rather, such a claim is based on the tort principle of enterprise liability. [9] As such, a threshold requirement for contributory infringement is proof of actual direct infringement by another. [10]

A contributory copyright infringer is: “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.” [11] Most courts, particularly in the internet context, have decided contributory copyright infringement cases based on this three-part test of (1) direct infringement, (2) knowledge, and (3) material contribution. [12] This formulation, however, appears nowhere in the Supreme Court's only contributory copyright infringement case. [13] In *Sony Corporation of America v. Universal City Studios*, the Supreme Court conflated the rules for contributory copyright infringement and vicarious copyright infringement. [14] The *Sony* Court also imported the “staple article of commerce” doctrine from patent law into the discussion of secondary copyright infringement liability [15] which has been imported into the knowledge requirement of the contributory copyright infringement analysis. [16]

A. Knowledge Requirement

Although no one would dispute that actual knowledge [17] satisfies the knowledge requirement of contributory copyright infringement, it is unclear whether constructive knowledge satisfies this requirement. [18] The *Sony* Court clearly stated that “[t]here is no precedent in the law of copyright for the imposition of vicarious liability” based on the defendant's having “constructive knowledge of the fact that its customers may ... make unauthorized copies of copyrighted material.” [19] Many courts, however, have been willing to impose liability for contributory copyright infringement based on constructive knowledge. [20] Although the Seventh and Ninth Circuits disagree as to how *Sony*'s “staple article of commerce” doctrine should be applied, [21] they both have held that the doctrine affects the knowledge requirement: [22] if the technology is found to be “capable of substantial non-infringing uses” [23] (or, in the Seventh Circuit, if such uses are found to be probable), [24] then the complaining party must establish actual, and not constructive, knowledge on the part of the accused party. [25]

B. Material Contribution Requirement

The material contribution requirement has rarely been defined or elaborated upon in the case law since *Gershwin Publishing v. Columbia Artists Management*. [26] *Religious Technology Center v. Netcom On-line*
Communication Services stated simply that the secondary infringer's “participation must be substantial,” [27] and other courts have interpreted this element in terms of “but for” causation (i.e., that the infringement would not have occurred but for the contribution of the secondary infringer). [28] A similar interpretation of the material contribution element that has been gaining acceptance in recent internet cases was established in Fonovisa v. Cherry Auction, which looks at whether the secondary infringer provided “the site and facilities” for direct infringement. [29] This site and facilities test is the result of the tendency to conflate the requirements for contributory and vicarious copyright infringement. [30] The Ninth Circuit recently addressed the confusion, framing the rule more specifically: “provision of site and facilities for infringement, followed by a failure to stop specific instances of infringement once knowledge of those infringements is acquired.” [31]

III. DIGITAL MILLENNIUM COPYRIGHT ACT SAFE HARBOR PROVISIONS

When Congress passed the Digital Millennium Copyright Act (DMCA) to implement the provisions of the World Intellectual Property Organization (WIPO) Treaty and strengthen copyright protections in the digital realm, [32] there was concern that the new provisions, and the recent enforcement of intellectual property rights in the internet context, would open online service providers to considerable liability for infringement occurring in the context of the provision of their services. [33] Congress therefore sought to strike a balance in which service providers and intellectual property rights holders would cooperate in the enforcement of intellectual property rights online against actual repeat infringers and those who traffic in technologies that enable infringers to circumvent the technological self-help measures of intellectual property rights holders. [34]

To encourage the cooperation of online service providers and prevent a chilling of ISP investment in internet structure, [35] Congress enacted safe harbors for ISPs and other online service providers. [36] The OCILLA safe harbor provisions of the DMCA insulate service providers from liability for infringement due to the automated performance of their services for infringing customers. [37] Congress structured these safe harbors such that a service provider that knowingly contributes to a customer's infringement is liable whereas one that is unaware is exempt. [38] The goal of these provisions is not only to insulate providers from potential liability but also to provide them with a consistent and predictable legal framework under which to evaluate their risk of potential liability. [39] Congress did not intend to change the existing rules of copyright law, [40] but rather sought to offer the safe harbor liability limitations as an incentive for online service providers to cooperate with rights holders to protect intellectual property rights in the digital realm. [41] Thus, the procedures Congress envisioned for a judicial determination of contributory copyright infringement liability in light of the DMCA safe harbors were, first, a determination of infringement liability based on existing rules of law, and second, a determination of safe harbor eligibility. [42]

To prevent the chilling of internet investment, Congress enacted the provisions of the DMCA with a deliberately broad definition of “service provider.” [43] Section 512(k)(1)(B) defines a service provider in very general terms as “a provider of online services or network access, or the operator of facilities therefor.” [44] This broad definition encompasses ISPs but also web site owners [45] and the distributors of peer-to-peer and other networking software. [46] However, § 512(k) also contains a more specific definition of “service provider,” which refers specifically to ISPs and which applies only to the safe harbor for transitory network communications under § 512(a). [47] This distinction is evidence of a congressional intent to place ISPs in a separate category from, and to grant ISPs more protection than, other online service providers (like web site providers and software distributors).

A. Threshold Requirements Under § 512(i)

In order to be eligible for any of the OCILLA safe harbors under § 512(a)-(d), a service provider must satisfy the threshold requirements under § 512(i):

The limitations on liability established by this section shall apply to a service provider only if the service provider--

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers .... [48]
Congress intended this provision to require ISPs to provide notice and warning to their subscribers that flagrant repeat infringers face “a realistic threat of losing [their internet] access.” [49] In accordance with the face of the statute and its legislative history, courts have generally interpreted the provision as focused on the relationship between a service provider and its subscribers, and not affecting any of the following: [50] the knowledge requirement of contributory copyright infringement, [51] the “no monitoring” provision in § 512(m), [52] or the notice and takedown provisions under § 512(b)-(d). [53]

B. No Monitoring Required Under § 512(m)(1)

The legislative history and the text of the statute are clear that service providers have no affirmative duty to monitor their networks or servers for infringing content. [54] Section 512(m) specifies that “[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on ... a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.” [55] Although this provision has the obvious effect of reducing the burden on ISPs, it was actually enacted to protect the privacy of internet users. [56] Regardless of the purpose, this provision clearly places no duty upon service providers to monitor or police the content on their networks, and the lack of such monitoring does not affect a service provider's eligibility for the safe harbors under § 512(a)-(d).

C. Limitations on ISP Liability Under § 512(a)-(d)

There are four safe harbor provisions under § 512, relating to different operations of service providers. [57] The first applies to transitory network communications, the second to system caching, the third to information that users store on a server, and the fourth to search utilities. [58] Of the four, only the last two contain provisions regarding the so-called “red flag” test. [59]

The legislative history's discussion of a red flag test for service providers under the knowledge requirements of § 512(c)(1)(A)(ii)-(iii) adds some confusion to the straightforward no monitoring provision in § 512(m)(1). [60] This red flag test also confuses the otherwise clear notice and takedown provisions of § 512(b)-(d). [61]

The red flag test seems to be the statute's answer to the problem of willful blindness, operating in the grey area between the no monitoring provision [62] and the formal notice and takedown provisions. [63] Congress summarized the test as follows: “if the service provider becomes aware of a ‘red flag’ from which infringing activity is apparent, it will lose the limitation of liability if it takes no action,” [64] and the statute adds that, in response to a red flag, a service provider must act “expeditiously to remove, or disable access to, the [infringing] material.” [65]

In addition to the red flag test, the statute also contains express “notice and takedown” provisions. Only three of the four safe harbors under § 512 contain notice and takedown provisions; there are no such provisions in the safe harbor for transitory network communications. [66] These provisions detail specific procedures for a copyright holder to formally notify a service provider of the availability of infringing material on the provider's network and to have such material removed. [67] Among other things, the notice and takedown provisions require that service providers appoint a designated agent for receiving such notice, and that the providers make the agent's contact information available on their websites and provide it to the Copyright Office. [68]

Furthermore, subsection (n) specifies that, with respect to the four safe harbor limitations on liability in subsections (a)-(d), the red flag test and notice and takedown procedures do not apply to any subsection which does not expressly provide for them:

Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection. [69]

Therefore, the knowledge and notification requirements of the four safe harbors can be summarized as follows:
<table>
<thead>
<tr>
<th>Safe Harbor</th>
<th>Provider</th>
<th>Monitoring</th>
<th>Red Flag Test</th>
<th>Notice/Takedown</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) transitory</td>
<td>ISP &amp; OSP</td>
<td>not required</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b) system caching</td>
<td>OSP</td>
<td>not required</td>
<td>not applicable</td>
<td>does apply</td>
</tr>
<tr>
<td>(c) user-stored</td>
<td>OSP</td>
<td>not required</td>
<td>does apply</td>
<td>does apply</td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d) search utilities</td>
<td>OSP</td>
<td>not required</td>
<td>does apply</td>
<td>does apply</td>
</tr>
</tbody>
</table>

Glancing at this table, the congressional intent becomes clear: there is an almost absolute immunity from liability for transitory network communications; there is only liability for system caching if the provider fails to respond to formal notice of infringing content; and a service provider may be liable for user-stored information and content indexed with search utilities if infringing activity is apparent to the provider.

Although courts have generally been faithful to these distinctions, problems can arise in determining the proper category for a given service; this is particularly true with respect to Usenet. [70] A Usenet post could technically be described as information stored at the direction of a user because the user initiates the message that is (temporarily) stored on the ISP's server. [71] Because of the history of the legislation, however, Usenet posts are considered transitory network communications. [72] The legislative history indicates that § 512(a) was intended to codify the holding in *Netcom*, which dealt specifically with Usenet posts. [73] Usenet posts are not considered user-stored information primarily because they are propagated automatically and are only retained for a limited period of time. [74] Therefore, due to the legislative history of the DMCA and the nature of Usenet, courts have accepted that Usenet posts are transitory network communications and thus fall under the § 512(a) safe harbor. [75]

IV. JUDICIAL ENFORCEMENT OF CONTRIBUTORY INFRINGEMENT CLAIMS AGAINST ISPS

One example of a Usenet case, which was decided under the proper safe harbor category, but which is problematic for other reasons, is the Ninth Circuit case *Ellison v. Robertson*. [76] In this case, Robertson scanned some of the works of science fiction writer Harlan Ellison and posted them on the Usenet group alt.binaries.e-book. [77] The works were then automatically propagated to AOL's servers, which were set to retain posts for fourteen days. [78] An unknown period of time later, when Ellison learned of the posts, his counsel sent a § 512(c)(3) notice to AOL and another ISP via e-mail. [79]

Because AOL had recently changed its copyright infringement notification e-mail address, the e-mail was never received. [80] The address change was updated with the Register of Copyrights, and AOL's copyright web page

Copyright (c) 2006 Boston College Intellectual Property & Technology Forum, David Ludwig
contained the updated e-mail address, but Ellison's counsel was relying on the old address. [81] The reason the e-mail was never received is that AOL neglected to close the old e-mail account and forward incoming messages to the new account. [82] Eleven days after learning of the infringing content, Ellison filed a claim against AOL. [83] Upon receipt of the complaint, AOL disabled access to alt.binaries.e-book on its Usenet server. [84]

At summary judgment, the district court found a triable issue of fact as to whether AOL was a contributory copyright infringer [85] but granted summary judgment for AOL under the safe harbor provisions. [86] The Ninth Circuit reversed, finding triable issues of fact on both the contributory infringement and safe harbor parts of the analysis. [87] In its safe harbor analysis, the Ninth Circuit agreed that AOL is entitled to immunity from liability under § 512(a) but found a triable issue of fact as to whether AOL satisfied the eligibility requirements of § 512(i). [88]

The Ellison opinions are a good example of a DMCA case against an ISP. ISP cases are somewhat different from cases against other online service providers--specifically software providers [89] and web site owners [90]--even though, because of the broad statutory definition of a “service provider,” [91] all three are eligible for at least some of the safe harbors under the DMCA. Cases in which the accused party is a manufacturer and provider of peer-to-peer software are unique in that their software implicates the staple article of commerce doctrine. [92] Contributory copyright infringement claims against web site owners are distinct from claims against ISPs because web site owners generally do not perform any services that would qualify for the transitory network communications safe harbor under § 512(a). [93] The law of contributory copyright infringement and the DMCA safe harbor provisions have been applied differently in cases against these three types of defendants, sometimes resulting in a departure from the statutory guidelines or the applicable case precedent. [94]

A. Interpretation of Contributory Infringement

Since Sony, courts have been gradually broadening the knowledge and material contribution requirements for contributory copyright infringement, especially in the digital context. [95] This has occurred despite the clear congressional intent in enacting the DMCA to leave the existing law for contributory copyright liability unchanged. [96]

i. The Slippery Knowledge Requirement: From Sony to Netcom and Grokster

One of the most notable aspects of the evolution of contributory copyright infringement liability since Sony has been the broadening of the knowledge requirement to include constructive knowledge. [97] The Sony Court simply stated that constructive knowledge does not suffice for contributory infringement liability. [98] The expansion of the knowledge requirement in the internet context seems to have begun with the Netcom court's conflation of Sony's tests for vicarious and contributory infringement by incorporating an “ability to control” element into its knowledge analysis. [99] Despite this confused analytical framework, and also despite the fact that the Netcom court framed the knowledge requirement as “knew or should have known” (implying an acceptance of constructive knowledge), the court granted summary judgment for Netcom with respect to all infringing content posted on its servers prior to Netcom's receipt of actual notice of the infringing content. [100] The Netcom court did not mention Sony's staple article of commerce doctrine. [101]

Recently, the Seventh and Ninth Circuits have interpreted Sony's constructive knowledge prohibition and its staple article of commerce doctrine together, as meaning that constructive knowledge will suffice whenever the technology enabling the infringement is not capable of substantial non-infringing uses. [102]

One additional element that may affect the knowledge requirement, which was embraced by the Seventh Circuit in Aimster II, is the doctrine of willful blindness:

One who, knowing or strongly suspecting that he is involved in shady dealings, takes steps to make sure that he does not acquire full or exact knowledge of the nature and extent of those dealings is held to have a criminal intent. [103]
Although generally only applied in the criminal context, willful blindness is equated with implied knowledge, which is a type of actual knowledge. [104]

In the Ellison opinions, both the district court and the Ninth Circuit agreed that there was a triable issue of material fact that AOL had satisfied the knowledge requirement of contributory infringement. [105] These holdings are completely contrary to case precedent and are evidence of the judicial tendency to treat ISPs more harshly than other categories of alleged contributory infringers.

First, there is no evidence that AOL had actual, direct knowledge of the infringing content. Both courts accept as true that AOL never received Ellison's § 512(c)(3) notice e-mail. [106] Both courts also accept that AOL's failure to close its old copyright notification e-mail address and forward messages directed to that address was merely a negligent oversight and thus does not satisfy the intent requirements for willful blindness. [107] There is some evidence that months prior to the posting of Ellison's articles, AOL had received a phone call reporting the presence of other infringing materials on its Usenet service. [108] Even if such a report could be construed as constructive knowledge, constructive knowledge does not satisfy the knowledge requirement in this case because Usenet is clearly capable of actual non-infringing uses. Despite all of this, both Ellison courts refused to grant summary judgment to AOL on the knowledge requirement, finding a triable issue of fact that AOL had constructive knowledge of the infringing content. [109]

These Ellison knowledge holdings stand in direct contrast to the holdings in the software distributor and web site owner cases. In the Grokster software distributor case, decided by the Ninth Circuit only a few months after Ellison II, the court found the knowledge requirement not satisfied, despite actual knowledge, because Grokster did not have knowledge of the infringing activity at the time that they had the ability to control such activity. [110] Similarly, in the Hendrickson v. Amazon.com web site owner case, the court found that prior notice was no longer viable after a few months had passed. [111] These cases demonstrate the different judicial treatment of these three types of service providers with respect to the knowledge requirement of the contributory infringement analysis.

ii. Material Contribution as Given: Misreading Sony and Netcom

The Supreme Court did not expressly address the material contribution element in Sony, but Sony implies that simply providing a technology that is capable of substantial non-infringing uses, without also advocating the use of the technology for infringement, does not lead to secondary liability. [112]

The Netcom court expanded the material contribution requirement by defining it broadly as “substantial participation.” [113] In Netcom, the court did not specifically address the factual circumstances satisfying the material contribution requirement as distinct from the knowledge requirement; the court merely concluded that contributory copyright infringement liability can be fairly imposed on a service provider that is hosting a Usenet server if the service provider does not act to remove (or disable access to) the infringing material upon receipt of actual knowledge of the infringing content. [114]

Following the Ninth Circuit's opinion in Fonovisa, [115] courts began using the “site and facilities” test for evaluating the material contribution requirement. In A&M Records v. Napster, the Ninth Circuit equated the Netcom test, based on the failure to act after receipt of knowledge, with the site and facilities test. [116] The district court in Aimster I further equated the Napster test with “but for” causation; [117] but the court continued to note that this reading of the material contribution element was not necessary in the case at bar because there is evidence that Aimster expressly advocated the use of its technology for infringement. [118]

The Ninth Circuit clarified its prior readings of the material contribution requirement in Grokster: “material contribution can be established through provision of site and facilities for infringement, followed by a failure to stop specific infringement once knowledge of those infringements is acquired.” [119] This represents a slight retreat from the prior expansion of the material contribution element, but it is still a broader rule than the “express advocacy of infringement” test implied by Sony. One thing that both these formulations have in common, however, is that both imply some level of intent on the part of the accused contributory infringer: Sony's express advocacy implies intentional action; Netcom/Grokster's failure to act after receipt of knowledge implies intentional inaction.
In the *Ellison II* case (against an ISP), the Ninth Circuit quoted the full *Netcom* rule (i.e., that material contribution is satisfied by providing a Usenet server and failing to act upon receipt of knowledge), but then applied it, in the summary judgment proceeding at bar, as a per se rule against Usenet providers: “The *Netcom* court held that the fact that the Usenet service allowed Netcom's subscribers access to copyrighted works was sufficient to raise a triable issue regarding material contribution.” [120] In doing so, the *Ellison II* court removed the intent requirement from the *Netcom/Grokster* test and held that there was a triable issue of fact as to the material contribution element, [121] despite the fact that the court concedes that AOL did not have knowledge of the infringement (and thus could not have failed to act upon receipt of knowledge). [122] This outcome stands in stark contrast with the Ninth Circuit's very different interpretation of this same material contribution element in its *Grokster* decision, issued only a few months after the *Ellison II* opinion.

B. Application of the DMCA Safe Harbor Provisions

The *Ellison II* ISP case was not only anomalous for its reading of the elements of contributory copyright infringement; it also represented a departure from established law in its application of the DMCA safe harbor provisions. Both *Ellison* courts followed the legislative intent and case precedent in recognizing that Usenet hosting falls under the provision for transitory network communications, § 512(a), and not the provision for information stored by a user, § 512(c). [123] The appellate court, however, disagreed with the district court that AOL was entitled to summary judgment under the safe harbor provisions. [124] The Ninth Circuit held that there was a triable issue of fact as to whether AOL satisfied the threshold eligibility requirements under § 512(i). [125] Specifically, the court questioned whether AOL's repeat infringer policy had been “reasonably” implemented because AOL neglected to close its old copyright notification e-mail address and forward the messages to the new address. [126]

i. Misreading the Threshold Requirements

The legislative history of the § 512(i)(1) repeat infringer policy threshold requirement indicates that this requirement is directed to the relationship between a service provider and its subscribers and not to the relationship between a service provider and a complaining copyright holder. [127] This is apparent both from the congressional discussions of the threshold requirements, [128] as well as from the elaborate red flag and notice and takedown provisions in § 512(b)-(d), which specifically detail procedures for communications between a service provider and a complaining copyright holder. [129] Reading the “reasonably implemented” repeat infringer policy requirement of § 512(i) as affecting the procedures for appointing and maintaining contact information for receipt of notice by complaining copyright holders, as the Ninth Circuit did in *Ellison II*, renders all of § 512(c)(2) moot. [130]

Furthermore, the overarching legislative purpose of the DMCA was to create consistency in the application of liability so that service providers would know when they were opening themselves to potential liability for their actions in the digital realm. [131] Although the face of the statute and the legislative history may be less than clear as to the specific requirements of § 512(i)(1), [132] the *Ellison II* holding undermines the goal of consistency by departing from existing precedent in its strict reading of the § 512(i)(1) requirement and refusing summary judgment when AOL was clearly entitled to safe harbor protection as a matter of law. [133]

Although the case precedents interpreting § 512(i) do not all agree with one another, none of the prior case law implies a reading as strict as the Ninth Circuit's in *Ellison II*. In stark contrast, the district court's opinion in *Ellison I* represents the most lax reading of § 512(i) to date, concluding:

Subsection (i) does not require AOL to actually terminate repeat infringers, or even to investigate infringement in order to determine if AOL users are behind it. That is the province of subsection (c) .... Subsection (i) only requires AOL to put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights. [134]

The *Perfect 10 v. Cybernet Ventures* court took a slightly stricter approach in its § 512(i) analysis than the *Ellison I* court, but still maintained that a lack of user account termination in “instances where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users” is required.
for a finding that a repeat infringer policy was not reasonably implemented. [135] *Aimster I* held that § 512(i)(1) was not satisfied because the architecture of the Aimster service was such the repeat infringer policy could not possibly be implemented. [136] Finally, *Perfect 10 v. CCBill* held that “Congress requires reasonable implementation of a repeat infringer policy rather than perfect implementation,” and found that the accused party had reasonably implemented its repeat infringer policy even though it had not disabled a user's access even after a number of general notifications of infringement. [137]

In contrast to the above line of cases (against mostly web site owners and a software provider), which differ somewhat in their interpretation of the § 512(i) requirements, the Ninth Circuit adopted a more draconian interpretation in applying the requirements to an ISP in *Ellison II*. In that case, AOL met all the requirements set forth in the above cases, but the Ninth Circuit nonetheless found a triable issue of fact as to whether AOL’s repeat infringer policy had been reasonably implemented simply because “AOL should have closed the old e-mail account or forwarded the e-mails sent to the old account to the new one.” [138] In so holding, the court has not only departed from precedent and the legislative goal of consistency, but it has also read a stricter version of the notice provisions of § 512(c) into both the threshold requirements of § 512(i) and the substantive requirements for the safe harbors under § 512(a)-(b). This holding results in the court's absurd conclusion that AOL does qualify for safe harbor under § 512(a), but may not be eligible for such because it has not satisfied the threshold requirements of § 512(i). [139]

ii. Willful Blindness and § 512(m)(1)

Although not expressly mentioned by the court, the Ninth Circuit's absurd holding in *Ellison II* seems to be based on the specter of willful blindness: that an ISP may change its copyright infringement e-mail address, and purposefully delay in closing the old account and forwarding the messages directed to it, simply in order to allow infringing activity to take place and avoid liability. Judge Posner of the Seventh Circuit explored similar concerns in *Aimster II*. In that case, in response to Aimster's argument that it did not have knowledge of the infringing activity because all of the files transferred via its software were encrypted, the Seventh Circuit employed the doctrine of willful blindness [140] to conclude that “a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used.” [141] This raises a question as to the relationship between the prohibition on willful blindness and the § 512(m) no monitoring provision.

Section 512(m) says that the availability of the safe harbors is not conditioned on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.” [142] Reading this provision in light of the definition of willful blindness [143] implies exactly what the red flag test [144] stipulates: if the service provider has some knowledge (understood as either direct knowledge or implied knowledge [145]), then it has a duty to investigate.

This understanding of the relationship between willful blindness and the no monitoring provision accords with the Seventh Circuit's application of the willful blindness doctrine against a software provider in *Aimster II*, [146] but is contrary to the Ninth Circuit's holding against an ISP in *Ellison II*. [147] The Seventh Circuit found that Aimster knew that its software was used for primarily infringing purposes [148] and held that the fact that each particular infringing transmission was encrypted was not sufficient to excuse Aimster from liability, under the willful blindness doctrine. [149] Based on the factual findings of Aimster's knowledge of infringing activity, the Seventh Circuit did not impose a burden on Aimster that violated the no monitoring provision of § 512(m).

The Ninth Circuit in *Ellison II*, however, seems to have applied the willful blindness doctrine in contradiction to the no monitoring provision. In that case, the court denied summary judgment to AOL simply because AOL had changed its copyright address and failed to promptly close the old account and forward messages directed to the old account. [150] If the facts had been different, this may have been a proper application of the willful blindness doctrine, but here, the Ninth Circuit did not contest the district court's factual finding that “AOL did not have actual knowledge of the infringement before being served by Ellison.” [151] Therefore, the court seems to have used the willful blindness doctrine in order to impose an affirmative duty to monitor upon the ISP.

In short, in *Ellison II*, the Ninth Circuit was penalizing AOL solely because changing a copyright infringement
e-mail address and not immediately following up (by closing the old account and forwarding messages from the old account to the new) is something that another service provider might do in order to turn a blind eye to copyright infringement. [152] The Ninth Circuit was literally holding AOL out as an example to prevent future willful blindness on the part of ISPs. [153]

V. SHOOTING THE MESSENGER: WHY ISP LIABILITY IS THE WRONG ANSWER

The Ninth Circuit Ellison II case exemplifies the judicial tendency to hold ISPs to a higher standard of liability for contributory copyright infringement than other service providers (like web site owners and software distributors). The court's impulse to do so seems to make some sense: ISPs are the gatekeepers of the internet--they control users' access to the internet and, as such, are in a unique position to control online copyright infringement. [154] Such an impulse, however, runs contrary to Congress's express intent in enacting the DMCA, and the Supreme Court has cautioned other courts that the expansion of copyright protections is a task best left to Congress. [155]

There are compelling public policy concerns that argue for adherence to the congressional mandate. The internet is significantly benefits the public by both subsidizing public discourse and fostering the growth of e-commerce. Furthermore, the existence and growth of the internet is dependent in large part on ISPs, who both invest in the structure of the internet and provide affordable access to a rapidly growing number of users. As with prior technological innovations -- such as newspapers, telephones, and broadcast and cable television--the internet subsidizes and creates a unique forum for public discourse. [156] Furthermore, because the internet is also an expansive commercial forum, it represents a unique realm that merges speech and commerce.

Both public benefits of the internet--speech and commerce-- enrich intellectual property owners. A robust public discourse fuels intellectual creation and serves as free advertising for the commerce in intellectual property. Furthermore, Congress noted that “a thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment.” [157] As such, the free flow of information on the internet is ultimately to the benefit of intellectual property rights holders.

VI. CONCLUSION

The unique role that ISPs play within the context of cyberspace means that they are crucial to the growth and expansion of the internet, but they are also particularly susceptible to contributory copyright infringement liability. In § 512, Congress considered the position of ISPs and crafted legislation which would protect the growth of the internet without sacrificing the protection of intellectual property rights holders. The judicial inclination to hold ISPs to a higher standard than other online service providers, however, undermines the delicate balance struck by Congress. Courts need to remain faithful to the letter and intent of the DMCA in order to facilitate the dual congressional goals of encouraging growth and investment in the internet and also protecting intellectual property rights.


[1]. Throughout this paper, I use the term “ISP” in reference specifically to the narrow category of internet “gatekeepers”: providers, like America Online and EarthLink, which enable end-users to connect to the internet, and which also usually provide auxiliary services like web site and e-mail hosting and Usenet newsgroup access. This definition is distinct from the statutory definition of a “service provider” under 17 U.S.C. § 512(k)(1)(B)--sometimes referred to as “Online Service Providers” or “OSPs”--a category broad enough to include web site owners and other internet content providers.

[2]. The specific role of ISPs in the context of the internet is as follows:

Direct control over communications over the Internet rests with the Internet service providers (ISPs) who own the individual networks that, in the aggregate, comprise the Internet. The effectiveness of this confederation of
networks rests on ISPs' decisions to adopt a particular suite of standard networking protocols—Internet Protocol (IP) and Transport Control Protocol (TCP) are its highest-profile members—that allow end users to be indifferent to the configuration of the networks between their computers. IP, in particular, operates on the assumption that any computer that receives a communication will forward that message to the next computer on the route to its ultimate destination. So far, participants in large IP networks have generally transmitted other participants' messages without further examination of their source or content, exactly as if they were common carriers. This rule of universal mutual message forwarding is essential to Internet end users' ability to create and use sophisticated communications applications without concerning themselves with the details of the network routes that connect their computers.


[5]. Section 1201 imposes criminal penalties for the circumvention of technological protections preventing access to, or copying of, copyrighted works, without a license from the copyright holder; or trafficking in access control circumvention technologies. 17 U.S.C. § 1201 (1999).

[6]. Section 512(h) describes the mechanism by which a copyright holder can, under certain circumstances, seek a subpoena that forces an ISP to divulge the identity of its infringing users. 17 U.S.C. § 512(h) (1999).

[7]. See Part III.C, infra.


[9]. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996); Nimmer, supra note 8, at § 12.04[A][2].


[11]. Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162(2d Cir. 1971); Nimmer, supra note 8, at § 12.04[A][3][a].

[12]. See, e.g., Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004) [hereinafter Ellison II]; Metro-Goldwyn-Mayer Studios v. Grokster Ltd., 380 F.3d 1154, 1160 (9th Cir. 2004) [hereinafter Grokster].


[14]. See Sony, 464 U.S. at 434-39. See also Netcom, 907 F. Supp. at 1373-74 (conflating the tests for contributory and vicarious liability in its contributory liability analysis); Jesse M. Feder, Is Betamax Obsolete?: Sony Corp. of America v. Universal City Studios, Inc. in the Age of Napster, 37 Creighton L. Rev. 859, 875 (2004) (noting that Sony did not discuss “the individual elements of contributory infringement”). Vicarious copyright infringement liability, which is based on the tort doctrine of respondeat superior, is imposed where the secondary infringer (1) possessed “the right and ability to supervise the infringing conduct” and (2) received a direct financial benefit from the infringement. Nimmer, supra note 8, at § 12.04[A][2]; See also Napster, 239 F.3d at 1022; Fonovisa, 76 F.3d at 261-62.
[15]. Sony, 464 U.S. at 440-42; See also discussion at notes 21-24, infra. The “staple article of commerce” doctrine in patent law states “that the sale of a ‘staple article or commodity of commerce suitable for substantial noninfringing use’ is not contributory infringement.” Id. at 440 (quoting 35 U.S.C. § 271 (c)). The Sony Court phrased the copyright version of the doctrine as follows: “the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.” Id. at 442.

[16]. The Seventh and Ninth Circuits, however, are split as to how the staple article of commerce doctrine should be applied to the knowledge requirement. Compare Grokster, 380 F.3d at 1162 (holding that the technology must merely be capable of substantial non-infringing uses); In re Aimster Copyright Litigation, 334 F.3d 643, 649-51 (7th Cir. 2003) [hereinafter Aimster II] (holding that the technology must be capable of substantial non-infringing uses and that such uses must be probable). See Amicus Curiae Brief of the American Intellectual Law Association in Support of Neither Party at 3-9, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd. (2004) (No. 04-480), available at http://thlnk.com/aipla/Grokster.Amicus.Brief/719; See also discussion at notes 21-24, infra.

[17]. There are two types of “actual knowledge”: direct knowledge and implied knowledge. See Part IV.A.i, infra.


[19]. Sony, 464 U.S. at 439 (emphasis added). Curiously, this language was quoted completely out of context by the Ninth Circuit and thereby made to imply the exact opposite. Compare Napster, 239 F.3d at 1020, with Sony, 464 U.S. at 439.

[20]. See Ellison II, 357 F.3d at 1077 (stating the rule as “knew or had reason to know,” then applying it as “should have been on notice”); Netcom, 907 F. Supp. at 1374 (using “knew or should have known” standard); Sega Enters. Ltd. v. MAPHIA, 857 F. Supp. 679, 686-87 (N.D. Cal. 1994) (conflating knowledge requirement with material contribution requirement); See also Mark A. Lemley & R. Anthony Reese, Reducing Digital Copyright Infringement Without Restricting Innovation, 56 Stan. L. Rev. 1345, 1357 (“it is not clear that Sony itself would have escaped secondary liability under the Ninth Circuit's reading of the Supreme Court's test”). The trend of broadening the knowledge requirement established in Sony is discussed in Parts IV.A.i and IV.B.iii, infra.

[21]. See note 16, supra.

[22]. Grokster, 380 F.3d at 1162; Aimster II, 334 F.3d at 649-51.

[23]. Sony, 464 U.S. at 442.


[25]. See note 22, supra. See also note 17, supra.

[26]. 443 F.2d 1159.


[29]. Fonovisa, 76 F.3d at 264 (concerning retailers selling infringing materials at a swap meet; concluding that “it would be difficult for the infringing activity to take place in the massive quantities alleged without the support service provided by the swap meet” including “the provision of space, utilities, parking, advertising, plumbing, and
customers”). See also Grokster, 380 F.3d at 1163 (applying the site and facilities test); Napster, 239 F.3d at 1022 (affirming the district court's application of the site and facilities test); Netcom, 907 F. Supp. at 1373-74 (finding that Netcom “not only leases space but also serves as an access provider”).

[30]. See discussion at note 14, supra.

[31]. Grokster, 380 F.3d at 1163 (following Fonovisa and Netcom).


[35]. See Evans, supra note 2, at 449 (“If ISPs are exposed to liability for forwarding others' messages [which is the very nature of all internet communications] ... the norm of universal mutual message forwarding that underlies the present operation of the Internet will be threatened.”)


[42]. See generally Ellison II, 357 F.3d at 1077-81 (employing these procedures); Napster, 239 F.3d at 1019-25 (employing these procedures); Aimster I, 252 F. Supp. 2d at 649-61 (employing these procedures); Ellison v. Robertson, 189 F. Supp. 2d 1051, 1057-72 (C.D. Cal. 2002) (“Ellison I”) (employing these procedures).


[46]. See generally Aimster II, 334 F.3d 643, 658; Napster, 239 F.3d 1004.

[47]. 17 U.S.C. § 512(k)(1)(A) defines a “service provider” as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, or material of the user's choosing, without modification to the content of the material as sent or received.” See also Part III.C, infra, for a discussion of the safe harbor for transitory network communications under § 512(a).

[48]. 17 U.S.C. § 512(i)(1). Section 512 also lists the additional requirement that the ISP “accommodates and does not interfere with standard technical measures,” a requirement that has not spurred any litigations and which is not material to the current discussion. 17 U.S.C. § 512(i)(1)(B).


[51]. See Part II.A, supra.

[52]. See Part III.B, infra.

[53]. See Part III.C, infra.


[56]. H.R. Rep. No. 105-551, pt. 2, at 64 (“New Section 512(l) [later renumbered as § 512(m)] is designed to protect the privacy of Internet users.”).


[59]. Compare 17 U.S.C. §§ 512(c)(1)(A)(ii)-(iii), (d)(1)(B)-(C) (red flag provisions under subsections (c) and (d)), with 17 U.S.C. § 512(a)-(b) (not containing similar red flag provisions).

[60]. See H.R. Rep. No. 105-551, pt. 2, at 53-54; See also Evans, supra note 2, at 466 (noting that the red flag test “coexist[s] uncomfortably” with the no monitoring provision).


[63]. See Part III.B, infra. See generally Zarins, supra note 18.


[67]. The notice and takedown procedures are codified in 17 U.S.C. § 512(c)(2)-(3), and are applied to the safe harbors in §§ 512(b)(2)(E), (c)(1)(C), (d)(3). Provisions for counter-notice and replacement of material previously removed appear in 17 U.S.C. § 512(g).


[70]. Usenet, short for “user network,” is “the world's biggest electronic discussion forum,” which employs a bulletin board format. Preston Gralla, How the Internet Works 107 (7th ed. 2004). Discussions are organized into “newsgroups,” grouped by subject. Id. at 55. There is no single network or server that is the Usenet. Id; Ellison I, 189 F. Supp. 2d at 1053 n.2. When a user posts a message to Usenet, the user's Usenet server automatically transmits and distributes the message to Usenet servers worldwide. Gralla at 108-09; Ellison I, 189 F. Supp. 2d at 1054. America Online (AOL) has estimated that its Usenet servers receive “more than twenty-four million messages each week.” Ellison I, 189 F. Supp. 2d at 1054.

[71]. See generally Gralla, supra note 74, at 107-09.


[73]. Id.

[74]. See Ellison II, 357 F.3d at 1075 (“AOL's policy was to store and retain files attached to USENET postings on the company's servers for fourteen days); Evans, supra note 2, at 458 (“Because of the high volume of traffic on Usenet, most system administrators limit retention of messages to two weeks or less.”)

[75]. Ellison II, 357 F.3d at 1081; Ellison I, 189 F. Supp. 2d at 1070.

[76]. 357 F.3d 1072.

[77]. Ellison II, 357 F.3d at 1075.

[78]. Id. For a discussion of Usenet architecture, see note 70, supra.

[79]. Ellison II, 357 F.3d at 1075.

[80]. Id.

[81]. Ellison II, 357 F.3d at 1080.

[82]. Id.

[83]. Ellison II, 357 F.3d at 1075.

[84]. Id.

[85]. Ellison I, 189 F. Supp. 2d at 1060.

[86]. Ellison I, 189 F. Supp. 2d at 1072.

[87]. Ellison II, 357 F.3d at 1081-82.

[88]. Id.

[89]. See generally Grokster, 380 F.3d 1154; Aimster II, 334 F.3d 643; Napster, 239 F.3d 1004.

[90]. See generally ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001); Amazon, 298 F. Supp. 2d 914; eBay, 165 F. Supp. 2d 1082.
[91]. See discussion at note 43, supra.

[92]. See generally Grokster, 380 F.3d 1154; Aimster II, 334 F.3d 643; Napster, 239 F.3d 1004. See also Parts II, II.A, supra.

[93]. See note 90, supra. See also discussion at note 47, supra.

[94]. See Parts IV.A, B, infra.

[95]. See Parts IV.A.i, ii, supra.


[97]. “Knowledge,” in the legal sense, is divided into two types: actual knowledge and constructive knowledge. Black's Law Dictionary 393-94 (2d Pocket Ed. 2001). Furthermore, there are two types of actual knowledge: direct/clear knowledge and implied/reasonable knowledge. Id. Direct knowledge is often indicated by the term “known”; implied knowledge is often indicated by the term “reason to know”; and constructive knowledge is often indicated by the term “should have known.” Id.

[98]. See discussion at note 19, supra.


[100]. Netcom, 907 F. Supp. at 1374.

[101]. Netcom, 907 F. Supp. 1361. See also Parts II, II.A, supra.

[102]. Grokster, 380 F.3d at 1162; Aimster II, 334 F.3d at 649-51. Or, in the Seventh Circuit, if such uses are probable. Aimster II, 334 F.3d at 649-51. See Parts II.A, supra.

[103]. Aimster II, 334 F.3d at 650. See also Part IV.B.iii, supra.


[105]. Ellison II, 357 F.3d at 1077; Ellison I, 189 F. Supp. 2d at 1058.

[106]. Ellison II, 357 F.3d at 1077; Ellison I, 189 F. Supp. 2d at 1057.

[107]. See Ellison II, 357 F.3d at 1077, 1080; Ellison I, 189 F. Supp. 2d at 1057-58.

[108]. Ellison II, 357 F.3d at 1077; Ellison I, 189 F. Supp. 2d at 1058. The evidence was a phone call to AOL's customer service department, months prior to the posting of Ellison's work, generally reporting the presence of infringing works by other authors on the Usenet system. Id.

[109]. Ellison II, 357 F.3d at 1077; Ellison I, 189 F. Supp. 2d at 1058.

[110]. Grokster, 380 F.3d at 1162.


[114]. See Id.

[115]. See Fonovisa, 76 F.3d 259. See also discussion at note 29, supra.

[116]. Napster, 239 F.3d at 1022.


[118]. Id. (following the logic of Sony, but not citing it as representing this principle).

[119]. Grokster, 380 F.3d at 1163 (combining the tests from Netcom and Napster).

[120]. Ellison II, 357 F.3d at 1078.

[121]. Id.

[122]. Ellison II, 357 F.3d at 1077-78.

[123]. Ellison II, 357 F.3d at 1081; Ellison I, 189 F. Supp. 2d at 1067-72. See discussion at note 72, supra.

[124]. Ellison II, 357 F.3d at 1082.

[125]. Id.

[126]. Ellison II, 357 F.3d at 1080, 1082. See also 17 U.S.C. § 512(i)(1).


[128]. Id.


[130]. See Ellison I, 189 F. Supp. 2d at 1066 n.15 (concluding that using subsection (i) to import the notice and takedown requirements of subsection (c) into subsections (a) and (b) would upset the delicate balance struck by Congress); See also 17 U.S.C. § 512(n) (clearly stating that the requirements of one subsection of the statute do not apply to any other subsection). Incidentally, by notifying the Copyright Office of the new e-mail address and updating the e-mail address on its web site, Ellison II, 357 F.3d at 1077, AOL was in full compliance with the requirements of § 512(c)(2); although, it should be noted, compliance with these requirements is not even required for safe harbor protection under § 512(a). The fact that AOL had initially delayed in updating this information, is immaterial to the Ellison case because the information had been updated by the time Ellison's counsel tried to contact AOL. Id.


[132]. See Cybernet, 213 F. Supp. 2d at 1176; Nimmer, supra note 8, at §§ 12B.02[B][2]-[3].
It may be argued that since this was merely a summary judgment proceeding, AOL would achieve the proper result at trial. The fact that AOL is required to submit to an expensive trial on the merits in order to establish the result that is clear as a matter of law, however, is reason enough to address this anomalous holding. In fact, it is clear that the burden of a trial was a cost that AOL deemed unreasonable, as the case recently settled. See the joint press release filed by the parties announcing the settlement, available at http://www.authorslawyer.com/c-ellison.shtml.

[134]. Ellison I, 189 F. Supp. 2d at 1066.


[138]. Ellison II, 357 F.3d at 1080.

[139]. Ellison II, 357 F.3d at 1082.

[140]. See discussion at note 103, supra.

[141]. Aimster II, 334 F.3d at 650-51.


[143]. See discussion at note 103, supra.

[144]. See discussion at note 63, supra.

[145]. See note 97, supra.

[146]. See Aimster II, 334 F.3d at 650-51.

[147]. See Ellison II, 357 F.3d at 1080-82.

[148]. Aimster's online instructional tutorials and its Club Aimster service both displayed infringing titles and were thus both evidence that the manufacturers knew that their software was being used for infringing purposes. Aimster II, 334 F.3d at 646, 651-52.

[149]. Id. at 650-51.

[150]. Ellison II, 357 F.3d at 1080.

[151]. Ellison I, 189 F. Supp. 2d at 1058.

[152]. See Ellison I, 189 F. Supp. 2d at 1058 (“If AOL could avoid the knowledge requirement through this oversight or deliberate action, then it would encourage other ISPs to remain willfully ignorant in order to avoid contributory copyright infringement liability.”)

[153]. See David L. Hudson, Jr., ‘Safe Harbor’ Under Fire, 3 No. 7 A.B.A. J. E-Report 4 (2004) (“Copyright experts say one lesson from the [Ellison II] case is that ISPs must be careful in ensuring they jump through the necessary safe harbor hoops.”)
[154]. It has been argued, however, that the services performed by ISPs are similar to telecommunications providers, and thus that ISPs should be granted the virtually unconditional statutory limitation of liability available to such common carriers. See Evans, supra note 2, at 448.

[155]. Sony, 464 U.S. at 431.
