Washington Journal of Law, Technology & Arts

Volume 1 | Issue 3 Article 3

8-2-2005

A Few Degrees Off the Mark: Miniature Missteps That Can Render the Safe Harbors of the DMCA Inaccessible

Nicole J. Nyman

Corporate & Commercial
Cite as: Nicole J. Nyman, *A Few Degrees off the Mark: Miniature Missteps that Can Render the Safe Harbors of the DMCA Inaccessible*, 1 Shidler J. L. Com. & Tech. 11 (Aug. 2, 2005), *at* <http://www.lctjournal.washington.edu/vol1/a011Nyman.html>

A FEW DEGREES OFF THE MARK: MINIATURE MISSTEPS THAT CAN RENDER THE SAFE HARBORS OF THE DMCA INACCESSIBLE

By Nicole J. Nyman[1]

ABSTRACT

The term Internet Service Provider ("ISP"), as defined by the Digital Millennium Copyright Act ("DMCA"), includes virtually any online service. These services are eligible for safe harbor protections under the DMCA when they fulfill certain enumerated requirements. However, minor missteps can leave ISPs unprotected and exposed to liability for copyright infringement. This Article will discuss, through a survey of recent cases, several such mistakes made by ISPs and tips to avoid them.

TABLE OF CONTENTS

INTRODUCTION

<1> Every mariner knows the importance of exact calculations when charting a course to sail. Even being just a few degrees off the mark can result in missing the desired destination by many miles and remaining adrift and vulnerable on open waters. Similarly, in a legal context, the safe harbors of the Digital Millennium Copyright Act ("DMCA")[2] are only attained by those which do not make even minor mistakes in charting their course

of action.

<2> In 2004, the United States Court of Appeals for the Ninth Circuit handed down a decision in *Ellison v. Robertson*[3] , in which America OnLine ("AOL") was left outside of the safe harbors of the DMCA and rendered vulnerable to charges of copyright infringement. AOL made one small misstep. It changed an email address without message forwarding. This seemingly trivial mistake left it outside the safe harbor and exposed to huge liability.

<3> This Article will first examine what entities are considered ISPs under the DMCA and the requirements for the protection of the safe harbors. The remainder of the discussion will focus on missteps that an entity should avoid in order to benefit from the safe harbors and avoid costly litigation regarding copyright infringement.

ISP DEFINITION AND REQUIREMENTS

<4> As an incentive to cooperate with copyright owners combating infringement, the DMCA provides special protections to Internet Service Providers (ISPs). Section 512 of the Act[4] creates safe harbors that limit ISP liability when the infringer is a subscriber of that Internet service and is using it in the course of infringement. These safe harbors provide a defense against infringement charges when the service provider (1) acts as a conduit for infringing material,[5] (2) caches infringing material,[6] (3) stores infringing material at the direction of a user,[7] or (4) provides access to infringing materials, often through a link or search reference.[8]

<5> The term "service provider" under the DMCA has a much broader meaning than the colloquial use of the word, extending far beyond such entities as AOL, Verizon, and MSN. As defined by the DMCA, a "service provider" is "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[9] For the purposes of most safe harbors, the definition is further expanded to any service which is a "provider of online services or network access, or the operator of facilities therefore."[10]

<6> The term "service provider" has been interpreted very broadly by the courts and has been found to reach beyond the traditional ISPs, such as America Online, to entities such as online auction sites, online age verification services, and file

sharing services.[11] In considering the two definitions of a service provider, the *In Re Aimster Copyright Litigation*[12] court noted that "[a] plain reading of both definitions reveals that 'service provider' is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the definitions."[13] Thus, the safe harbors of § 512 are available to the majority of companies with Internet activities if they act consistently with the requirements of the DMCA.

<7> In order to qualify for the safe harbors and obtain protection from financial liability, the ISP must meet the eligibility requirements laid out in § 512(i). The ISP must (1) adopt a policy that provides termination of subscribers who are repeat infringers, (2) inform the subscribers regarding the policy, and (3) reasonably implement the policy. All three conditions must be met in order to qualify for the safe harbor protections; however, it is the third condition where ISPs often fall short. Of the reported cases discussing requirements for safe harbor protections, the contested issue is virtually always whether the company took the steps necessary to "reasonably implement" the policy. To avoid litigating such issues, ISPs should be aware of the easily avoidable missteps that other ISPs have made to lose safe harbor protections.

REVIEW AND UPDATE FREQUENTLY

<8> The most easily avoidable misstep is that of AOL in *Ellison v. Robertson*.[14] There, the infringer scanned an author's works and posted them on a newsgroup. This led to the forwarding of these files to servers throughout the world, including some AOL servers. These servers stored the documents for a period of two weeks, during which time there were available to AOL subscribers. When Ellison, the author, learned that his copyright was being infringed, he notified AOL of the infringing activity according to the DMCA guidelines, thereby putting AOL on notice. AOL alleged it never received the notification and learned of the infringement only upon the receipt of Ellison's complaint, at which time AOL promptly blocked subscriber access to the newsgroup containing the infringing material. Although the district court granted AOL's motion for summary judgment, the Ninth Circuit reversed the district court's application of the safe harbor limitations. The case was remanded because there were triable issues of material fact to determine whether AOL met the § 512(i) requirements.

<9> So, what was the small misstep? Although AOL had a policy in place against repeat infringers and informed its subscribers of the policy, there remained a question of whether AOL had

"reasonably implemented" their policy as required by § 512(i). The evidence showed that the reason AOL did not receive the first email notification from Ellison was simply because it changed the address to which these notifications were to be sent. However, AOL did not forward messages sent to the old address or notify senders that the old address was inactive. Since the messages sent to the old account were not forwarded to the new account, they were simply lost "into a vacuum."[15] According to the court, that fact alone may be sufficient to find that AOL had not "reasonably implemented" their policy and may expose them to liability for the copyright infringement. Something as simple as failing to forward email could turn into a large judgment against AOL.

<10> There are many small details similar to this which are easily overlooked in daily business operation. However, companies should identify details that can result in liability and create procedures to ensure that those details are not overlooked. Companies should also periodically review the company policies and the underlying enforcement mechanisms. Through this, they will become aware of necessary updates and avoid oversights that may result in trouble for the company.

AVOID SELF-IMPOSED OBSTACLES

<11> Another aspect of company action that ISPs should evaluate is whether they have placed any obstacles in the way of enforcing their repeat infringer policy. It is not enough for an ISP to have a policy and inform users if they then make it impossible to reasonably implement the policy. These obstacles may range from purposeful disassociation of user identities from the material posted on a message board to the failure to store transactional data for a adequate amount of time.

<12> An extreme example of self-imposed obstacles is *In re Aimster Copyright Litigation*,[16] where the court found Aimster liable for copyright infringement, notwithstanding its comprehensive repeat infringer policy. Aimster's policy contained specific information on procedures used to track and disable repeat infringers, what would happen in the event of mistakes in termination, and even had a form which could be filled out in order to alert Aimster of copyright infringement. The court agreed that Aimster had adopted a repeat infringer policy and there was ample evidence that they had notified subscribers of that policy. However, the court said Aimster was not eligible for the safe harbor provisions of the DMCA because it did not meet the "reasonably implement" requirement of § 512(i). In fact, the court said the policy was not implemented at all and was "an

absolute mirage"[17] because the encryption scheme that Aimster put in place made it impossible for them to implement the policy. While Aimster could determine which users had copyright-protected content on their hard drives, it was impossible for them to determine which files were being transferred by which users. Since Aimster chose to encrypt all communications between users, they had no ability to know when infringement occurred. "Adopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an 'implementation' as required by § 512(i)."[18]

<13> While ISPs likely are not in such an extreme situation and their self-placed obstacles may be less obvious than the encryption in *Aimster*, it would seem a reasonable extension that any company-placed obstacles which prevent the enforcement of the repeat infringement policy may rob the company of safe harbor protection.

SEND THE NECESSARY MESSAGE TO INFRINGERS

<14> Yet another issue to consider when reasonably implementing a policy is the message which company actions send to copyright infringers. The court in *Costar Group Inc. v. Loopnet, Inc.*[19] , in deciding whether the § 512 safe harbors should apply to the defendant, examined legislative history. It noted that the requirement of having and reasonably implementing a user policy is "designed so that flagrant repeat infringers, who abuse their access to the Internet through disrespect for the intellectual property rights of others should know there is a realistic threat of losing… access."[20] Although the defendant had the necessary policy firmly in place, the court would not grant summary judgment on the issue because it was unclear whether the defendant had actually terminated access of users who became repeat infringers. The court indicated that the purpose of the reasonably implement requirement was not only to make the infringed material unavailable, but to send a message to repeat infringers.

<15> Thus, a company must carefully evaluate the message their actions send to infringers. While less drastic action is required for first-time offenders, simply deleting the infringing material from the system will not be sufficient for repeat infringers. Instead, a realistic threat of access termination is also a necessary part of the equation. While there is no definitive authority on what creates this realistic threat, a provider could best avoid costly litigation by strictly enforcing its policy. Removing content acts only as a quick slap on the hand for

those users who repeatedly violate the policy provisions and is not sufficient to garner safe harbor protection.

DOCUMENT ENFORCEMENT MEASURES

<16> One final step in assuring DMCA safe harbor protection is found beyond the enforcement of the repeat infringer policy. Even when the ISP has a policy, informs users of such, and reasonably implemented the policy, this still may not be enough. Should litigation regarding policy implementation arise, it is also the responsibility of the ISP to show documentation demonstrating enforcement. Thus, ISPs should keep records of all users whose rights have been terminated and the details of those processes in order to have the evidence necessary to prove reasonable implementation of their policy in court.

<17> The ISP in *Perfect 10, Inc. v. Cybernet Ventures, Inc.*[21] did not enjoy safe harbor protection although they had a repeat infringer policy in place and had advised subscribers of the policy. The court found little likelihood that the provider would be able to enter in the safe harbors of the DMCA because it did not appear Cybernet "reasonably implemented" the policy. Although Cybernet asserted that it had taken action against infringing subscribers, there was no documentary evidence of such action. The court, by repeatedly referring to this lack of evidence[22] , made it clear that the service provider is saddled with the burden to bring forth evidence of "reasonable implementation" in order to qualify for safe harbor protections. If a service provider cannot provide evidence of reasonable implementation of the repeat infringer policy, there is "little likelihood that it can avail itself of Section 512's safe harbors."[23]

CONCLUSION

<18> Because the definition of ISP is extremely broad, the safe harbor protections provided by the DMCA are available to most companies with Internet services. Finding rest in these safe harbors often hinges on whether the ISP "reasonably implemented" a repeat infringer policy. In charting the course of company action, a misstep as minor as forgetting to forwarding email messages can leave an ISP outside the safe harbor and exposed to hefty liability for copyright infringement. ISPs should frequently evaluate their actions to assure they avoid simple errors which translate into unreasonable implementation of their repeat infringement policy.

PRACTICE POINTERS

From a survey of recent cases addressing the subject, the following are pointers for avoiding the errors which other ISPs have made:

- Review the company policy regularly and ensure that all measures are up-to-date and all information provided to third parties is current.
- Avoid ambivalence regarding user identities or other self-placed obstacles in the way of effective policy enforcement.
- Assure the policy and its enforcement send the message to users that they will likely loose access as a result of engaging in repeat infringement.
- Document the steps taken to enforce a repeat infringer policy, including users whose accounts have been terminated and information showing the promptness of such termination.

<< Top

FOOTNOTES

1. Nicole J. Nyman, University of Washington School of Law, Class of 2005. Many thanks to Mary Heuett Oemig for feedback on a draft of this Article.
2. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304 (1998) (codified in various section of 17 U.S.C.).
3. 357 F.3d 1072 (9th Cir. 2004).
4. 17 U.S.C. § 512 (2005).
5. 17 U.S.C. § 512 (a) (2005).
6. 17 U.S.C. § 512 (b) (2005).
7. 17 U.S.C. § 512 (c) (2005).
8. 17 U.S.C. § 512 (d) (2005).
9. 17 U.S.C. § 512(k)(1)(A) (2005).
10. 17 U.S.C. § 512(k)(1)(B) (2005).
11. *See* Bruce P. Keller & Jeffrey P. Cunard, *Copyright in the Digital Age*, 754 Practicing Law Inst./Pat. 293, 352 (2003) (discussing "service provider" definition

and citing illustrating cases).

12. 252 F.Supp.2d 634 (N.D. Ill. 2002).
13. *Id*. at 658.
14. 357 F.3d 1072 (9th Cir. 2004).
15. *Id.* at 1080.
16. 252 F.Supp.2d 634 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).
17. *Id*. at 659 n.18.
18. *Id*. at 659.
19. 164 F.Supp.2d 688 (D. Md. 2001).
20. *Id*. at 703.
21. 213 F.Supp.2d 1146 (C.D. Cal. 2002).
22. *Id*. at 1178.
23. *Id*. at 1179.

<< Top