Neighborhood Watch: The Negation of Rights Caused by the Notice Requirement in Copyright Enforcement Under the Digital Millennium Copyright Act

*Colin Folawn**

> Unlike traditional media that limit and pre-censor the content of information disseminated to the public, the Internet could become the digital equivalent of the classic agora where public debate, artistic creativity, and cultural diversity coexist with commercial transactions. Realization of that possibility depends on our ability to strike an equitable balance between the public interest in access to works and rightholders' ability to profit from their investments in producing such works. —*Deborah Tussey*[1]

I. INTRODUCTION

This Comment discusses the problems inherent in the notice requirement[2] of the Digital Millennium Copyright Act (DMCA),[3] which requires copyright holders to notify Internet Service Providers (ISPs) before they are required to remove infringing material from a server or investigate a copyright infringement incident. Although some copyright holders[4] have sufficient resources to detect infringement and enforce their rights through the DMCA, the structure of the notice requirement represents a heavy burden to stakeholders like independent copyright holders. Because they are unable to effectively

---

* J.D. *summa cum laude*, Seattle University School of Law, 2003; B.M., Willamette University, 1996. The author thanks the staff of the *Seattle University Law Review* for their fellowship, commitment to legal scholarship, and tireless editing during a landmark year. He also thanks his family for their support of his law school endeavors. The author dedicates this Comment to his wife, Jocelyn Folawn.

1. Deborah Tussey, *From Fan Sites to Filesharing: Personal Use in Cyberspace*, 35 GA. L. REV. 1129, 1132 (2001).

2. 17 U.S.C. § 512(c) (1998).

3. Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

4. For example, the Recording Industry Association of America (RIAA) is a large organization that assists and represents most major recording companies in lobbying, litigation, and public relations efforts relating to copyright infringement.

enforce copyrights, independent copyright holders experience a negation of rights.

Additionally, the substantial compliance standard is confusing because the courts do not seem to understand how to balance the competing interests as Congress intended. As will be discussed later, one recent memorandum opinion offers hope for sorting out these interests properly.[5] To recalibrate the balance of these competing interests, Congress should consider the metaphor of a neighborhood in regulating Internet copyrights.

The Neighborhood Watch Program was developed by the National Crime Prevention Council (NCPC) to detect and prevent crime, but it was also meant to strengthen communities by empowering residents to take active roles in protecting themselves.[6] After the September 11, 2001 terrorist attacks, the Program has taken on a new relevance, and the NCPC is addressing the epidemic of fear by expanding the number of participating neighborhood groups.[7] Strangely enough, the Internet,[8] a neighborhood of its own,[9] does not have a cognate to the Neighborhood Watch Program, even though an epidemic of its own, in the form of copyright infringement[10] and other criminal activity,[11] has been taking place for years. Although the DMCA[12] was a

---

5. *See infra*, Part IV (B), discussion of *In re* Verizon Internet Services, Inc., 240 F. Supp. 2d 24 (D.D.C. 2003).

6. National Crime Prevention Council, *Neighborhood Watch Gets Residents Prepared, available at* http://www.ncpc.org/ncpc/ncpc/?pg=5882-3200-5232-6106 (last visited Mar. 1, 2003).

7. *Id.*

8. Initially spawned as a military communications tool known as DARPANet (Defense Advanced Research Project Agency Network), the first Internet was a distributed networking model, which enabled communication between any two connected points, even in the event of a nuclear attack. *See A Bit of Internet History, available at* http://www.firstbite.co.nz/training/intro/history.html (last visited Feb. 10, 2002) (stating that "The history of the Internet began with the RAND group in 1966. Paul Baran was commissioned by the US Air Force to do a study on how it could maintain its command and control over its missiles and bombers, after a nuclear attack. Baran's finished document described several ways to accomplish this task. What he finally proposed was a packet switched network. This network would have no central hub, and no central control centre. Instead it would have lines linking various places together. Packets would be forwarded from place to place until they arrived at the proper destination.").

9. *See generally*, Julian Dibbell, *A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 1994 ANN. SURV. AM. L. 471 (1994), *reprinted in* MARK STEFIK, INTERNET DREAMS 293 (MIT Press 1997); Pavel Curtis, *Mudding: Social Phenomena in Text-Based Virtual Realities, in* MARK STEFIK, INTERNET DREAMS 265 (MIT Press 1997).

10. *See* Charles C. Mann, *The Year the Music Dies, available at* http://www.wired.com/wired/archive/11.02/dirge.html (last visited Mar. 4, 2003); *see also* Todd Woody, *The Race to Kill Kazaa, available at* http://www.wired.com/wired/archive/11.02/kazaa.html (last visited Mar. 4, 2003).

11. *See, e.g.*, Michelle Delio, *Why Worm Writers Stay Free, available at* http://www.wired.com/news/politics/0,1283,49313,00.html (Dec. 27, 2001); Declan McCullagh & Ryan Sager, *FBI Blasts Reluctant Hackees, available at* http://www.wired.com/news/

step in the right direction (albeit initiated by private interests),[13] it failed to adequately address the concerns of independent copyright holders,[14] who are unable to maintain their rights. Equally concerning is the difference of opinion among the courts in determining how strict compliance with the notice requirement should be.[15]

At first glance, the notice requirement[16] of the DMCA seems to correctly place the burden on the copyright holders because, as owners or authors of the work, they are the beneficiaries of copyright protection, and they are best able to identify instances of infringement. However, after examining the nature of modern file sharing software and recent case law, it becomes clear that the resources required to find infringement on the Internet and to create this notice are overly burdensome to independent copyright holders.

The problem of unauthorized file sharing via the Internet is seen clearly in the realm of digital music.[17] The advent of file compression

---

politics/0,1283,43451,00.html (May 1, 2001); Michelle Delio, *Brit Cops Tackle E-Thievery, available at* http://www.wired.com/news/business/0,1367,43171,00.html (Apr. 19, 2001); Katie Dean, *Who Should Fight Cybercrime?, available at* http://www.wired.com/news/politics/0,1283,36566,00.html (Jun. 1, 2000); Polly Sprenger, *US Senate Cracked Again, available at* http://www.wired.com/news/politics/0,1283,20180,00.html (Jun. 11, 1999); Douglas Thomas, *How Much Damage Did Mitnick Do?, available at* http://www.wired.com/news/politics/0,1283,19488,00.html (May 5, 1999); Polly Sprenger, *AOL Fraud Touches West Virginia, available at* http://www.wired.com/news/politics/0,1283,18436,00.html (Mar. 13, 1999); Claudia Graziano, *Tracking Global Cybercrime, available at* http://www.wired.com/news/politics/0,1283,15222,00.html (Sep. 25, 1998); Michelle Delio, *MS Refocuses on Software Pirates, available at* http://www.wired.com/news/business/0,1367,49856,00.html (last visited Feb. 16, 2002); Declan McCullagh, *Cybercrime Bill Ups the Ante, available at* http://www.wired.com/news/politics/0,1283,50363,00.html (last visited Feb. 16, 2002).

12. Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

13. JESSICA LITMAN, DIGITAL COPYRIGHT 130 (2001).

> The Clinton administration had committed itself to a general game plan in connection with all Internet regulation that required it to identify what needed to be done to facilitate electronic commerce, to do that, and *to do as little as possible except for that.* After the bruising copyright fight in the last Congress, it wanted to satisfy the Hollywood and Silicon Valley communities but did not want to have to expend significant political capital.

Id. (emphasis added).

14. This Comment is concerned with copyright holders who are not affiliated with record companies that are represented by the Recording Industry Association of America (RIAA), because such artists do not likely have the resources to investigate, detect, and prevent copyright infringement of their works. Some independent copyright holders may allow the free and open sharing of their works in order to increase the works' popularity and value, but this Comment focuses on those copyright holders who may not choose to do this.

15. As the later analysis indicates, this not only requires an inquiry into what information is necessary for the ISP to locate the instance of infringement, but also an examination of the competing interests implicated by the notice requirement mechanism.

16. 17 U.S.C. § 512(c) (1998).

17. Jane Irene Kelly, *In Depth—The Download Dilemma, available at* http://www.newmedia.com/nm-ns.asp?articleID=2212 (last visited Nov. 10, 2001) (quoting

technology,[18] combined with the increasing popularity of broadband Internet service,[19] enables large amounts of copyrighted content to be shared with the world quickly, without the permission of the copyright holder and in violation of their copyrights. With the creation of online services like Napster,[20] the problem of music piracy grew large enough to receive the significant attention of the Recording Industry Association of America (RIAA), because millions of Internet users illegally shared millions of files on a daily basis.[21] Although the Napster network no longer functions as it once did, copyright infringement continues through peer-to-peer (P2P) technology, and the problem remains.[22] Without an adequate enforcement model, the neighborhood

---

Russell J. Frackman, Esq., in his opening argument in A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004 (9th Cir. 2001), "14,000 recordings are downloaded [per] minute using the Napster system."); *see, e.g.*, RIAA, *RIAA/Anti-Piracy Statistics, available at* http://www.riaa.com/Protect-Campaign-6.cfm (last visited Nov. 10, 2001) (stating that 2.8 million illegal recordable compact discs (CD-Rs) were seized in 2001, reflecting a 175% increase from CD-Rs seized in 2000).

18. *WinZip®—What is a Zip File Anyhow?, available at* http://www.winzip.com/aboutzip.htm (last visited Aug. 8, 2002) ("Usually the files 'archived' in a Zip are compressed to save space. Zip files make it easy to group files and make transporting and copying these files faster.").

19. Federal Communications Commission, *Deployment of Advanced Telecommunications Capability: Second Report*, (Aug. 2000), *available at* http://ftp.fcc.gov/Bureaus/Common_Carrier/Orders/2000/fcc00290.pdf (reporting that, as of Dec. 31, 1999, there were approximately 2.8 million subscribers to advanced or high-speed Internet access, which is defined as 200 kilobits per second or higher).

20. *A&M Records*, 239 F.3d at 1013–1016; *see also* Dan Labriola & David English, *Most Innovative Software: Napster, available at* http://www.zdnet.com/products/stories/reviews/0,4161,2662839,00.html (last visited Dec. 20, 2001).

21. *See* Labriola & English, *supra* note 20.

22. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 243 F.Supp. 2d 1073, 1081 (C.D. Cal. 2003). The court described the peer-to-peer file sharing system clearly:

> [T]he "Kazaa system" operates in a manner conceptually analogous to the Napster system . . . . [The Kazaa Media Desktop (KMD)] enables Internet users to search for and exchange digital media with other users . . . . Once installed, each KMD user may elect to "share" certain files located on the user's computer, including, for instance, music files, video files, software applications, e-books, and text files. When launched on a user's computer, KMD automatically connects to the FastTrack peer-to-peer network, and makes any shared files available for transfer to any other user's computer.
>
> Once connected to the FastTrack network, the KMD software provides a range of means through which a user may search through this pool of shared files. For instance, a user can select to search only among audio files, and then enter a keyword title or artist search. Once a search commences, the KMD software displays a list (or partial list) of users who are currently sharing files that match the search criteria, including data such as the estimated time required to transfer each file. The user may then click on a specific listing to initiate a direct transfer from the source computer to the requesting user's computer. When the transfer is complete, the requesting user and source user have identical copies of the file, and the requesting user may also start sharing the file with others.

of the Internet will continue to be plagued by criminal copyright infringement.

Additionally, the DMCA was the result of a legislative process that pandered to private interest groups like the RIAA and the ISP industry, rather than considering the rights of individual copyright holders.[23] This is evidenced throughout copyright law, where certain forms of expression are arbitrarily given protection, and others are excluded. For example, there is no rational reason that the Copyright Act of 1976 needed to protect an exclusive right to public performance for digital audio transmission, but not digital video transmission.[24] One of the resulting problems was the inequitable burden placed upon independent copyright holders to protect their copyrights. Under the DMCA, ISPs and Online Service Providers (OSPs) have no duty to search for infringing activities until they receive notification from the copyright holder or her designee.[25] Because these important considerations seem to have been neglected in the DMCA, this Comment proposes that the initial burden of locating infringement of copyrighted music over the Internet[26] should be shared between independent copyright holders and ISPs.[27] Independent copyright holders *qua* enforcing authorities are ill-equipped to meet the challenge of investigating unauthorized file sharing on the Internet. Instead, the DMCA should have been structured as to encourage cooperation among the various Internet stakeholders, not unlike the well-known Neighborhood Watch Program.[28] Finally, this Comment proposes that the government should not play a monitoring role, because it is institutionally incompetent to monitor the entirety of the Internet, and such an effort would likely be viewed as an unacceptable violation of consumer privacy.

The Proposal in this Comment may be more applicable to OSPs than it is to ISPs. For the purposes of the DMCA and the Proposal, the most important distinction is in the function they provide to

---

Id. *See also In re* Verizon Internet Services, Inc., 240 F.Supp 2d. 24, 35 (D.D.C. 2003) (stating that "the largest opportunity for copyright theft is through peer-to-peer ('P2P') software").

23. LITMAN, *supra* note 13, at 144–145.

24. 17 U.S.C. § 106(6) (2000).

25. *Id.* § 512(c)(3)(A)(i)–(vi); Joseph P. Zammit, *Website Liability: Risks and Costs of Compliance*, 611 PLI/PAT 815, 835 (2000).

26. This Comment refers to the World Wide Web (WWW), File Transfer Protocol (FTP), Usenet and other various Internet protocols, but it focuses on peer-to-peer file (P2P) sharing, arguably the most popular conduit for copyright infringement.

27. This Comment focuses on OSPs more than ISPs. This is appropriate because OSPs arguably derive a benefit from all consumer activity on their domains (including unauthorized file sharing), whereas an ISP may derive a lesser benefit as is discussed *infra*, Part V.

28. *See* National Crime Prevention Council, *Effective Strategy: Neighborhood Watch*, *available at* http://128.121.17.146/ncpc/ncpc/?pg=2088-9644 (last visited June 3, 2003).

Internet users and their role in maintaining the Internet. The DMCA defines a service provider, for the purposes of subsection (a), as "an entity offering the transmission, routing, or providing 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."[29] Simply put, ISPs provide consumers with service in the form of access to a network. The DMCA provides a second definition of service provider, applicable to all other subsections: "[A] provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."[30] At a minimum, OSPs do not supply access to the Internet itself, but they create services that can be reached through a pre-existing Internet connection. At the most, OSPs provide both online services and Internet access. Businesses that exist on the Internet add value because they create spaces of communication or commerce on the Internet, but they are generally much smaller in scope than ISPs. Nicholas Negroponte might refer to this distinction as the difference between the selling of access and the selling of bits themselves.[31]

Part II of this Comment explains why the DMCA was created, beginning with a brief discussion of modern copyright justifications. Part III lays out the mechanics of the notice requirement and the safe harbor protection for ISPs. Part IV focuses on inconsistencies among the courts and the enforcement dilemma posed by the DMCA. Part V proposes a different standard for the initial notice, encouraging ISPs to work cooperatively with independent copyright holders. This part includes a preview of services and software that exist and that are being developed to ease the burden of finding and managing digital content. Finally, Part VI analyzes the benefits and burdens created by the Proposal and addresses possible counterarguments that would likely be posed by the various stakeholders, and Part VII presents concluding remarks.

II. BACKGROUND AND PURPOSE OF THE DMCA

A. Copyright Law and the Internet

The law surrounding copyright infringement applies to activity within the Internet neighborhood because copyright does not depend on the environment in which a work exists. Intellectual property,

29. 17 U.S.C. § 512(k)(1)(A) (1998).
30. *Id.* § 512(k)(1)(B).
31. NICHOLAS NEGROPONTE, BEING DIGITAL 51–58, 62–67 (1996).

some of which is protected by copyright law, is often referred to as a "bundle of exclusive rights."[32] For copyright, the bundle includes exclusive rights to reproduce the work,[33] to distribute copies of the work,[34] to create derivative works,[35] and to perform or publicly display the work.[36] While the bundle of rights may change depending on the nature or character of the owned subject, these rights would not necessarily change simply because the work can be disseminated over a network.[37] After all, references to works in the Copyright Act of 1976 focus on the creation and type of work, not on how it is physically embodied.[38] Because copyright protection does not change simply because of the medium of a given work, such rights apply similarly in the real world and in cyberspace. Some commentators have correctly made the Internet seem more similar to the real world than it is unique.

In the beginning of *Code and Other Laws of Cyberspace*, Professor Lawrence Lessig aptly analogizes the post-Communist Russia of 1989 to the Internet of 1995.[39] Americans pressured those in Eastern and Central Europe to adopt constitutionalism, but such commands scared the former communists into a remarkably staunch anti-governmental posture.[40] Instead, a libertarian sensibility took over, allowing the markets and nongovernmental organizations to determine the course of the new country.[41] Unfortunately, this choice failed to protect against the kind of control the former communists feared. Power was transferred from governmental organizations to private interests like the Russian mafia.[42] Therefore, although systems of control were

32. Stewart v. Abend, 495 U.S. 207, 220 (1990).

33. 17 U.S.C. § 106(1) (2000).

34. *Id.* § 106(3).

35. *Id.* § 106(2).

36. *Id.* § 106(4)–(5).

37. Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1475 (1995).

38. 17 U.S.C. § 101 (2000) ("'Audiovisual works' are works that consist of a series of related images which are intrinsically intended to be shown by the use of machines, or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the works are embodied."). A work is protected under the Copyright Act of 1976 if it is an "original work of authorship fixed in any tangible medium of expression." 17 U.S.C. § 102 (2000). Advances in Internet technology have made the sharing of digital works very easy, and European countries have allowed for a private copying exception. Ginsburg, *supra* note 37, at 1477. However, the United States courts have refused such a rule. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013–1016 (9th Cir. 2001).

39. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 4 (1999).

40. *Id.* at 3.

41. *Id.* at 3–4.

42. *Id.* at 4.

changed by the decision not to create new laws and rules, such change failed to achieve the intended freedom.[43]

The consumer Internet is similar to post-Communist Europe because of the haphazard manner in which it was created. Not unlike the fall of Communism, the Internet arrived like an alarm call, and anti-governmental sentiment was present in both instances.[44] Professor Lessig stresses that Eastern Europe's problem should be a warning to those concerned with the future of the Internet, because without a constitutional build of rules and values for the Internet, power will reside solely with those who program the code of the Internet.[45] Finally, Professor Lessig voices this warning as an imperative, because there is "every reason to believe that cyberspace, left to itself . . . . will become a perfect tool of control . . . . The invisible hand, through commerce, is constructing an architecture . . . that makes possible highly efficient regulation."[46] Clearly, the application of law to the Internet neighborhood is not only possible, but also necessary in order to further the public good and prevent control by purely private entities. Congress likely saw this same need when it created the DMCA. More concretely, the role of copyright law is just as important to the real world as it is to the Internet.

Professor Jane C. Ginsburg[47] argued that copyright law should be applied regardless of whether the work exists in a digital or analog medium and regardless of its ability to be disseminated across a distributed network.[48] In other words, the package should not dictate the rights in the content. In this regard, the DMCA did not dilute copyrights in digital works. Therefore, although Professor Lessig might say that the law of code, which influences Internet user behavior on an organic level, is stronger than a law exterior to code, where the behavioral mandate is external to the user experience, both Professors Lessig and Ginsburg would likely agree that there is nothing about the Internet that necessarily rejects our conceptions of law in society. The same justifications and conceptual framework of rights, duties, powers, and liabilities apply—the Internet does not evade this time-tested logic; only its application differs. Moreover, the existence of the DMCA is strong evidence that Congress is not yet willing to let copyright evanesce. However, before delving into the structure of the

43. *Id.*
44. *Id.*
45. *Id.* at 5.
46. *Id.* at 5–6.
47. Ginsburg, *supra* note 37, at 1466.
48. *Id.* at 1467.

DMCA, it is important to examine the modern justifications of copyright protection.

B. Copyright Justifications

The U.S. Constitution provides that Congress has the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[49] Modern copyright law exists to maintain the delicate balance between incentives for creators and public access to their works.[50] Although the importance of the reward is a secondary concern to that of society's benefit,[51] the currently popular theoretical justification for copyright law is that it secures a monetary incentive for creators to continue to create, thereby enriching the public when the work is necessarily shared with the world.[52] To protect these rights, a copyright holder may bring an action for injunctive relief[53] or damages[54] for activity that infringes[55] the bundle of exclusive rights. However, the Copyright Act of 1976 did not contemplate the Internet, and additional legislation was needed.

C. Enter the DMCA

The DMCA was created to modernize traditional copyright law for the rapidly evolving Internet age.[56] Unlike copyright law,[57] the

---

49. U.S. CONST. art I., § 8, cl. 8.

50. Tussey, *supra* note 1, at 1131–32.

51. Fox Film Corp. v. Doyal, 286 U.S. 123, 127 (1932).

52. *See generally* Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105 (1990) (discussing these principles in the context of the fair use doctrine); *see also* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984) (stating that "[Copyright law] is intended to motivate the creative activity of authors . . . by the provision of a special reward, and to allow public access to the products of their genius after the limited period of exclusive control has expired.").

53. 17 U.S.C. § 502(a) (2000).

54. *Id.* § 504.

55. *Id.*

56. Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512, Pub. L. No. 105-304, 112 Stat. 2860 (1998); *see, e.g.*, Amy P. Bunk, *Validity, Construction and Application of the Digital Millennium Copyright Act*, 2001 A.L.R. Fed 2, 1 (2002) (unpublished annotation).

57. David A. Petteys, *The Freedom to Link?: The Digital Millennium Copyright Act Implicates the First Amendment in* Universal City Studios, Inc. v. Reimerdes, 25 SEATTLE U. L. REV. 287, 291–92 (2001):

> A copyright infringement suit was prosecuted simply by locating the producer of copies and obtaining an injunction to prevent further copying or by seizing his printing press. Not only was the infringer relatively static, but the cost of equipment presented a significant barrier of entry to the illicit trade of book pirating. Technology has radically altered the paradigm. The means of copying, a computer, is readily obtainable and allows the digital pirate to make near-perfect copies of digital audio and

DMCA contemplates the existence of the Internet, digital copying, and the liability of ISPs. Proponents of the DMCA said that it was "designed to facilitate the robust development and worldwide expansion of electronic commerce, communications, research, development, and education."[58] Among other aspects, the DMCA focuses on technological means of copyright infringement by outlawing the circumvention of copyright protection schemes,[59] the manufacture of technology for circumvention purposes,[60] and the dissemination of such technology.[61] In addition, Congress was careful not to change the basic structure of rights, remedies, and defenses within traditional copyright law.[62] Some commentators felt the DMCA was "exactly what the copyright law needed to maintain its relevance in today's Internet world."[63] Arguably, the DMCA maintained the ability for the Internet to evolve as unfettered as legally possible[64] while attempting to ensure that content creators still received incentives to create. The importance of the DMCA is better understood after briefly examining the reality of the Internet before its enactment.

The DMCA was necessary in order to solve the problem posed by the emergence of the consumer Internet. When compression and identification schemes were diverse,[65] the global sharing of digital works was splintered into discrete communities.[66] However, the MP3 file format (a colloquial abbreviation for Motion Picture Experts' Group Layer-3) soon emerged as a standard,[67] enabling any Internet user with a standard dial-up modem to share commercial music without having to pay for it.[68] Suddenly, digital entertainment content, including music, could be disseminated to the world instantaneously.[69]

> video works at very little cost . . . . Moreover, the Internet allows a copyright infringer to distribute perfect copies around the world instantaneously and anonymously.

Id.

58. S. Rep. No. 105-190, at 1 (1998).

59. 17 U.S.C. § 1201(a)(1)(A)–(D) (1998).

60. *Id.* § 1201(a)(2).

61. *Id.* § 1201(b)(1)(A)–(C).

62. *Id.* § 1201(c).

63. Christian C.M. Beams, *The Copyright Dilemma Involving Online Service Providers: Problem Solved . . . for Now*, 51 FED. COMM. L.J. 823, 825 (1999).

64. Namely, the DMCA allowed the evolution of the Internet to continue without abrogating other laws.

65. *See generally*, Farhad Manjoo, *Napster Sharers Sharing Less, available at* http://www.wired.com/news/culture/0,1284,42452,00.html (last visited Feb. 3, 2002).

66. Brad King, *File Tracker May Go Too Far, available at* http://www.wired.com/news/mp3/0,1285,43714,00.html (last visited Feb. 15, 2002).

67. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

68. *Id.*

69. Brad King, *File Trading Instantly Is Easier, available at* http://www.wired.com/news/mp3/0,1285,48071,00.html (last visited Feb. 15, 2002).

The average Internet user was endowed with worldwide distribution power equal or superior to that of the great publishing houses of the twentieth century, with one added bonus: virtual anonymity.[70] This anonymity was created partially because of the distributive nature of the Internet,[71] but more closely, it was unclear who was responsible for investigating and enforcing copyright law on the Internet.[72] Obviously, this created an entirely new problem for Congress: patching an old law to fit the unique digital environment of cyberspace.[73] The DMCA was an answer, albeit somewhat stilted and slow, to a real problem. One aspect of the DMCA, the notice requirement, appears innocuous and even beneficial, but it creates a caste system, negating the rights of independent copyright holders. Part III discusses the mechanics of the notice requirement.

III. THE NOTICE REQUIREMENT AND THE SAFE HARBORS

A. The Notice Requirement[74]

The notice requirement promulgated under the DMCA is unduly burdensome to independent copyright holders because they alone carry the initial burden of discovering unauthorized file sharing, unaided by any service providers. In the unlikely circumstance that a copyright holder is able to discover an incident of infringement, she must then satisfy the notice requirement in order to prompt the ISP to take action. This section discusses the mechanics of the notice requirement as promulgated under the DMCA.

An ISP is notified of infringement under the DMCA only if such notice is a written communication that substantially includes the following factors: (1) a signature (physical or electronic) of the copyright

---

70. Brad King, *ISPs Face Down DMCA*, *available at* http://www.wired.com/news/technology/0,1282,40816,00.html (last visited Feb. 12, 2002).

71. King, *supra* note 69.

72. *Id.*

73. LITMAN, supra note 13, at 111.

> The threat and promise of networked digital technology is that every individual with access to a computer will be able to perform the twenty-first-century equivalent of printing, reprinting, publishing, and vending. If the vast majority of them do not comply with the copyright law, then the copyright law is in danger of becoming irrelevant.

Id.

74. For a brief discussion of the substantial compliance problem, focusing on the *ALS Scan* case, see Pearson Liddell, Jr. & William D. Eshee, Jr., *Substantial Notice under the Digital Millennium Copyright Act*, 8 TEX. WESLEYAN L. REV. 379 (2002); for a more complete analysis of *ALS Scan*, see Laura Rybka, ALS Scan, Inc. v. Remarq Communities, Inc.: *Notice and ISPs' Liability for Third Party Copyright Infringement*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 479 (2001).

owner or his authorized agent;[75] (2) identification of the copyrighted work that is being infringed;[76] (3) identification of the material that is being infringed;[77] (4) information that is reasonably sufficient to allow the ISP to contact the complaining party;[78] (5) a statement that the copyright holder has a good faith belief that the use or activity is not authorized by law;[79] and (6) a statement that the notification is accurate and that the complaining party is authorized to act on behalf of the copyright holder under penalty of perjury.[80]

If the complaining party fulfills factors (2), (3), and (4), then factor (1) is required only when the ISP promptly makes an attempt to contact the notifier in order to assist in the receipt of the required information.[81] Notification of infringement does not affect analysis as to whether the ISP had actual or constructive knowledge of infringement.[82] This means that, without more, notice of infringement alone will not subject an ISP to liability simply because of the information in the notice. An ISP is also free from liability for infringement even if it provides access to infringing material through an automated search engine, provided that there is no actual or constructive knowledge that the material or activity is infringing.[83] Clearly, it is only after the copyright holder specifically pinpoints the infringing activity that an ISP is under a duty to act.

Although one might argue that this is an appropriate scenario because the copyright holder is in the best position to identify infringement, this process is cumbersome and, in most instances, is bound to fail because ISPs are diverse in the services they offer and the protocols they use.[84] The courts already appear to be confused as to whether every factor must be present or if a factor-based analysis should apply.[85] At bottom, this inconsistency reflects confusion as to the purposes of the DMCA and how the competing interests of the ISP industry and copyright holders should be balanced. As will be discussed in Part IV, one court has identified these competing inter-

75. 17 U.S.C. § 512(c)(3)(A)(i) (1998).
76. *Id.* § 512(c)(3)(A)(ii).
77. *Id.* § 512(c)(3)(A)(iii).
78. *Id.* § 512(c)(3)(A)(iv).
79. *Id.* § 512(c)(3)(A)(v).
80. *Id.* § 512(c)(3)(A)(vi).
81. *Id.* § 512(c)(3)(B)(i).
82. *Id.* § 512(c)(3)(B)(ii).
83. *Id.* § 512(d)(1)(A)–(C).
84. *See, e.g.*, Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (discussing eBay auction numbers); *see also* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (discussing the proprietary Napster network).
85. *Hendrickson*, 165 F. Supp. 2d at 1089 (stating that "[T]he notification must include 'substantially' the. . .six *elements*." (emphasis added)).

ests and characterized the limited liability as an exchange for the burden of assisting with copyright enforcement, but first an understanding of the safe harbor provision is necessary.

B. The Safe Harbors[86]

Put simply, ISPs are those who provide "online services or network access," or those who operate "facilities therefor."[87] Under the DMCA, ISPs enjoy large, sweeping immunity from copyright liability including monetary,[88] injunctive,[89] and equitable relief,[90] provided that the ISP does not initiate the transmission of infringing material,[91] select the material,[92] select the recipients of the material (unless the process was automated),[93] maintain a copy on the network for longer than would be ordinarily necessary for the connection,[94] or modify the material.[95] Essentially, if the infringing material exists on the network at the sole direction of users, and the ISP has no actual or constructive knowledge of the infringement, the ISP will be immune from liability.[96] ISPs, therefore, are Internet neighbors who have a disincentive to look for copyright infringement. This is referred to as a safe harbor within which the ISP is allowed to operate freely.[97] However, this safe harbor is not without its limits.

If the ISP receives a direct financial benefit from the infringement, or if it fails to remove or disable access to the infringing material, then the ISP loses its immunity from liability.[98] If the ISP actually ends up removing the material from a user's account or domain, the ISP is immune from liability, provided that it takes reasonable

---

86. For a more complete discussion of the safe harbor provisions, see Raphael A. Gutiérrez, *Save the Slip for the Service Providers: Courts Should Not Give Short Shrift to the Safe Harbors of the Digital Millennium Copyright Act*, 36 U.S.F. L. REV. 907 (2002); for a robust analysis on how the safe harbor provisions apply to P2P technology, see Giovanna Fessenden, *Peer-to-Peer Technology: Analysis of Contributory Infringement and Fair Use*, 42 IDEA 391 (2002); *see also* Heidi Pearlman Salon, *Liability Immunity for Service Providers—How Is It Working?*, 6.1 J. TECH. L. & POL'Y 1 (2000), *at* http://grove.ufl.edu/~techlaw/vol6/Pearlman.html (last visited May 4, 2003).

87. 17 U.S.C. § 512(k)(1)(B).

88. *Id.* § 512(a)–(d).

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* § 512(a)(1)–(5).

95. *Id.*

96. *Id.* § 512(c).

97. *Id.*

98. *Id.* § 512(d)(2)–(3).

steps to notify the user about the takedown,[99] gives counter notice to the copyright holder should the ISP replace the material in question, and replaces the material within fourteen days following receipt of the counter notice.[100]

Although safe harbor provisions appear on their face to be beneficial to the growth of the Internet, these provisions, when combined with a strict read of the notice requirements, encourage ISPs to sit idly by until a copyright holder pinpoints the exact location of an infringing activity and gives specific and particular notice to the ISP.[101] Even when a copyright holder is able to determine with specificity where such activity is taking place, the artist is often required to do exhaustive investigation in order prompt the ISP to remove the infringing link, file, or directory.[102] This wait-and-see ISP posture effectively negates the rights provided by copyright law. Having briefly discussed the notice requirement and safe harbor provisions of the DMCA, it is helpful to examine recent case law determining what constitutes substantial compliance. Although the case law on this aspect of the DMCA is sparse, the courts are applying this standard inconsistently.

IV. SUBSTANTIAL COMPLIANCE: INCONSISTENCIES IN RECENT CASE LAW

A. The "Factors as Elements" Approach

The DMCA requires merely substantial compliance of its notice requirement, but the United States District Court for the Central District of California failed to give this allowance adequate consideration. In *Hendrickson v. eBay*,[103] the court held that plaintiff's notification of infringement to online service provider eBay did not substantially comply with the factors necessary for effective notice listed in 17 U.S.C. section 512(c)(3).[104] In addition to illustrating the problem with allowing for substantial compliance, this case demonstrates the site-specific informational burden copyright holders face once infringement is discovered. Before giving its inappropriately elemental analysis, the court implied that the plaintiff failed to give the notice in writing.[105] However, in doing so, the court failed to discern the distinction Congress allowed for when it required a "physical or elec-

99. *Id.* § 512(g)(1)–(2).
100. *Id.*
101. King, *supra* note 70.
102. *See, e.g.*, Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal., 2001).
103. *Id.*
104. *Id.* at 1092.
105. *Id.* at 1089.

tronic signature."[106] This strict interpretation of the notice requirement continued throughout the opinion.

First, the court stated that plaintiff failed to include a statement indicating a good faith belief that the information in the complaint was accurate.[107] Although this would generally seem to be a low threshold requirement (such a statement could likely be inferred from the content, tone, and ultimate goal of the communication), the court was likely correct with regard to the plaintiff's original e-mail message.[108] After all, plaintiff's cursory five-line message appeared suspect because it requested "any and ALL information . . . on these criminals," rather than the simple request that eBay initiate a "takedown" on the allegedly infringing activity.[109]

Second, the court discussed the lack of an "under penalty of perjury" boilerplate on the written notification.[110] Finally, the court noted the absence of eBay identification numbers on plaintiff's notice.[111] On the face of the opinion, the court appeared to place the greatest weight on this final aspect. The court reasoned that while the plaintiff did identify some auction numbers in a discovery response, and this pre-dated the filing of the complaint,[112] the lack of a statement as to a good faith belief that the items were pirated and that the allegations were accurate made the notice invalid.[113] Interestingly enough, the court interpreted 17 U.S.C. section 512(c)(3)(A)(iii) to mean that the plaintiff had to include the specific auction numbers because this would show the OSP the specific location of the alleged infringement. This is specious reasoning because, although such information would significantly reduce eBay's burden of removing the auction listings, it effectively adds an unnecessary legal burden to the copyright holder's DMCA task list—unnecessary because the auction could still be located without the individual identification numbers. While the inclusion of such numbers would have helped eBay in locating the auction, the notice requirement does not require that the copyright holder give all information that could be helpful to the ISP—only information that identifies the material being infringed.[114] If other courts follow *Hendrickson*, the copyright holder must not only run his own investigation throughout the entirety of the Internet, but now he must also familiar-

106. 17 U.S.C. § 512(c)(3)(A)(i).
107. *Hendrickson*, 165 F. Supp. at 1089–90.
108. *Id.* at 1091.
109. *Id.* at 1091 n.11 (emphasis in original).
110. *Id.* at 1089.
111. *Id.* at 1090–92.
112. *Id.*
113. *Id.* at 1089–90.
114. 17 U.S.C. § 512(c)(3)(A)(iii).

ize himself with the eccentricities of each Web service or software client through which infringing activity takes place. Taken together with the *Hendrickson* opinion, the lack of litigation involving online copyright infringement is evidence that the burden of supplying notice is simply too great for independent artists who wish to reduce infringement of their copyrights.[115]

Inexplicably, the *Hendrickson* court seemed to disagree with the Fourth Circuit decision, *ALS Scan, Inc. v. RemarQ, Inc.*, which correctly noted that "the DMCA . . . allows notice by means that comport with the prescribed format only 'substantially,' rather than perfectly."[116] In *ALS Scan*, the copyright holder provided substantial notice even though there was no representative list of the infringed works (photographs). Instead, ALS Scan identified the addresses of the two Usenet newsgroups were defined by ALS Scan's name, asserted that virtually all of the images were ALS Scan's copyrighted material, referred the defendant to two Web addresses where the defendant could find pictures of the ALS Scan models and obtain copyright information, and noted that each photograph was marked with ALS Scan's name and copyright symbol.[117] Arguably, *Hendrickson* represents a departure from the reasoning in *ALS Scan*, because although each plaintiff provided locating information (Hendrickson gave specific user information, while ALS Scan merely gave the Usenet newsgroup address—a far less specific location, given that some of the photographs were not owned by ALS Scan), Mr. Hendrickson failed and ALS Scan, Inc. succeeded.

ALS Scan reflects a correct analysis of Congress's intent in creating the notice requirement. In this case, ALS Scan appealed from a district court ruling that granted RemarQ's motion to dismiss because ALS Scan failed to comply with the notice requirements set forth in section 512(c)(3)(A).[118] RemarQ argued that it remained under the protection of the DMCA's safe harbor provision because ALS Scan failed to identify with specificity the nearly 10,000 pictures that were the subject of unauthorized copying on the "alt.als" and "alt.binaries.pictures.erotica.als" newsgroups.[119] The court held that ALS Scan complied with the notice requirement where the plaintiff complied strictly with only two of the six requirements: (3) a list of infringing works contained on the newsgroups and (4) identification of

115. Specifically, those artists who are unaffiliated with large licensing conglomerates like the RIAA.

116. ALS Scan, Inc. v. RemarQ, Inc., 239 F.3d 619, 625 (2001).

117. *Id.* at 625.

118. *Id.* at 621

119. *Id.* at 620.

the "works in sufficient detail to enable RemarQ to locate and disable them."[120]

Although there is no evidence that ALS Scan provided RemarQ with Usenet message identification numbers, but instead merely supplied the newsgroup names, the court found this to be sufficient under section 512(c)(3)(A)(iii).[121] The court's analysis was certainly aligned with the DMCA in that it was "[i]n the spirit of achieving a balance between the responsibilities of the service provider and the copyright owner."[122] Although *ALS Scan* may be a good example of what substantial notice was intended to be, it is a poor example of the problem with the notice requirement because ALS Scan, Inc. was a well-established and thriving Internet business that had adequate resources to search for and detect infringement on the Web and Usenet.[123]

Because substantially compliant notice under the DMCA appears to have inconsistent results, creating a significant burden to copyright holders wishing to reduce the unauthorized sharing of their works, Part V of this Comment offers a proposed change to the notice requirement.

B. The Bargain Theory for Immunity from Liability

The *Hendrickson* holding reflects a strict standard for determining whether a copyright holder has provided substantially compliant notice. The court in In re *Verizon Internet Services, Inc.*[124] may not have come to the same conclusion because it recognized that the Congressional gift of immunity from liability was predicated on the condition that the ISP or OSP would cooperate to reduce online copyright infringement.

After *Hendrickson* was decided, the United States District Court for the District of Columbia had an opportunity to examine more closely the subpoena power of the DMCA, and this analysis required

120. *Id.* at 624.

121. *Id.* at 624–25.

122. *Id.* at 625.

123. A pre-DMCA case, Sega Enterprises Limited v. Maphia, 948 F. Supp. 923 (N.D. Cal. 1996), demonstrates this as well. The facts of *Sega* indicate that copyright holders can easily identify instances of infringement on the Internet, including bulletin board systems (BBS). *Id.* at 928. However, a closer look illuminates the special advantages that are unavailable to most copyright holders. Unlike the *pro se* plaintiff in *Hendrickson*, Sega was a leading manufacturer and distributor of video game systems and software. *Id.* at 926. More importantly, Sega did not discover the infringing activity through any sort of affirmative investigation carried on at its own expense; instead, the suit was brought only after Sega received an anonymous tip that pirated versions and unauthorized copies of its software were being distributed on the defendant's BBS. *Id.* at 927. It was only after this unexpected tip that Sega then directed one of its employees to gain access to the defendant's BBS and confirm the unlawful activity. *Id.* at 926.

124. 240 F.Supp. 2d 24 (D.D.C. 2003).

the court to study the broad purposes of the DMCA, the modern realities of file sharing, and the *quid pro quo* of ISP immunity from liability. The court decided in *Verizon* that the subpoena authority granted by the DMCA in 17 U.S.C. section 512(h) affected ISPs that had limited liability.[125] Although this issue did not directly involve the notice requirement of the DMCA, the court necessarily discussed the purpose behind limited liability for ISPs, and the memorandum opinion is therefore relevant to this discussion.

From the title of section 512,[126] the court correctly inferred that the DMCA was primarily designed to limit ISP liability stemming from the acts of individual customers.[127] Next, the court correctly interpreted the statute to create a safe harbor from liability for all monetary relief due to direct, vicarious, or contributory copyright infringement.[128] The greatest contribution of this opinion, however, was found in a footnote where the court articulated the bargain between the competing interests of ISP efficiencies and copyright law. After noting the burden that the subpoena power created for ISPs, the court said, "But *in exchange* for complying with subpoenas under subsection (h), *service providers receive liability protection* from any copyright infringement—direct or vicarious—by their users. Hence, *any additional burden is offset by that protection*, which, of course, is exactly the contemplation reflected in the structure of the DMCA."[129] In addition to creating this duality of interests, the DMCA fractionalized the enforcement role of the copyright property interest; thus, it deserves brief discussion.

C. The Splintered Enforcement Dilemma

Before proceeding further, it is necessary to examine the theory of property and the dilemma posed by the DMCA's splintering of the enforcement role. It is generally accepted that property is an abstract concept, not existing in the real world.[130] Indeed, it is a four-fold relation involving the owner, the owned, the authority that enforces the rights involved, and the world, against whom the rights are enforced.

---

125. *Id.* at 26.

126. The title of 17 U.S.C. § 512. reads: "Limitations on Liability Relating to Material Online."

127. *Verizon*, 240 F.Supp 2d. at 27.

128. *Id.* (citing S. Rep. No. 105-190, at 20 (1998)).

129. *Id.* at 34, n.6 (emphasis added).

130. *See, e.g.*, Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L. J. 16 (1913) (discussing property as being a relation between legal subjects); *see, e.g.*, Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L. J. 710 (1917).

This theory of property does not prevent the role of enforcing authority from being shared among multiple entities, nor does it prevent one of the entities from performing multiple roles. However, the splintering of the enforcement role negates these rights if sufficient barriers to detection are erected.

The safe harbor provision and notice requirement of the DMCA splinters the role of enforcing authority among three entities: copyright holders, ISPs, and the courts. Copyright holders must first provide notice under 17 U.S.C. section 512(c). ISPs then become an enforcing authority only when the aforementioned notice requirement is satisfied. The courts are the final enforcing authority, but only if the copyright holder brings an action for injunctive relief under 17 U.S.C. section 502(a). Under this scheme, the role of the ISP or the courts is conditioned on the successful identification and report by the copyright holder. Because their roles are conditional, ISPs have no affirmative duty to monitor their domains until the copyright holder provides notice of the infringement, as will be discussed below. Neither federal nor state governments necessarily play any role in actively searching for copyright infringement, but the law provides statutory remedies to the copyright holder in the event that infringement is specifically detected.[131] Thus, although three entities may each play a role in enforcing copyright, the responsibilities are not shared. The initial enforcing authority is the copyright holder, because he must first detect the infringement. Although unauthorized file sharing continues to be a major aspect of Internet use,[132] the DMCA places the burden fully on individual rights holders or their patron organizations to discover any and all infringing activities. Since the individual copyright holder is an ineffective enforcing authority, one of two theoretical outcomes emerges. Either Internet users at large become the initial enforcing authority by informing copyright holders of infringement on the Internet, or copyright protection of digital works is destroyed because there is no adequate enforcing authority to detect infringement. The history of shareware demonstrates that the latter is likely true.

Some may argue that Internet users at large are a capable enforcing authority for copyright because users receive a direct benefit from the public release of creative works, and that they will be willing to

131. 17 U.S.C. § 504(c) (1998).

132. Software & Info. Indus. Ass'n, *Doesn't Everybody Do It? Internet Piracy Attitudes and Behaviors*, (Fall 2001), *at* http://www.siia.net/divisions/content/pubs/kmpg.pdf (last visited June 19, 2003) (stating that "48% of those surveyed believed that everyone who uses the Internet violates copyright laws at some point; 41% believed that stricter copyright regulations should be promulgated").

consistently inform ISPs of copyright infringement.[133] This theory has not proven true. The change in protection schemes for shareware software demonstrates this well. Shareware is a system of property where the creator/owner of a piece of software, upon its release, immediately creates a conditional right for anyone to use the software temporarily.[134] Although the extent of this right varies among software engineers, many allow some perpetual, though often increasingly limited, use without paying any fees.[135] The system of shareware is premised on the theory that those who continue to use the software will eventually pay a predetermined fee (or sometimes whatever the user feels the software is worth).[136] This phenomenon surfaced in the early 1990s, and most of the payment schemes were either optional or encouraged by guilt-producing pop-up windows that would appear after a period of use.[137] Unfortunately, the honor system failed to get the kind of financial results that shareware authors hoped, and mandatory registration enveloped the industry with online services,[138] crippling schemes,[139] and copy protection. As the shareware example demonstrates, the diligence of Internet users appears to be an inadequate enforcing authority if copyright holders are to derive monetary rewards. Therefore, the individual copyright holder, not the Internet community at large, must guard his copyright alone. Having discussed the theoretical justifications for copyright, the practical motivations for the DMCA, and the enforcement dilemma for individual copyright holders, this Comment offers a Proposal to level the balance between the competing interests of low burdens and freedom from vi-

---

133. The DMCA does not necessarily support such a system because notice must substantially include the "physical or electronic signature of *a person authorized to act on behalf of the owner* of an exclusive right that is allegedly infringed." 17 U.S.C. § 512 (c)(3)(A)(i) (emphasis added). Surely, this would not include good Samaritan Internet users.

134. *What is Shareware?*, *at* http://www.semicolon.com/Shareware.html (last visited Feb. 10, 2002) (stating that, "with shareware, you actually use the software before you pay a cent").

135. *Id.*

136. *Id.* (stating that users "decide whether you want to keep the software. If you decide to keep it, you must pay for it—on your honor! But if you decide not to keep it, just delete it from your system and pay nothing.").

137. *Successful Shareware*, *available at* http://www.semicolon.com/ShareSuccess/Shareware5.html (last visited Feb. 10, 2002). "'Nagware' is software that keeps reminding you to pay up. Typically all it does is nag. It doesn't deny any functionality to unpaid users, it just tries to annoy them into paying. After paying, the user is given some way to stop the nagging."

138. For example, Kagi Software is one such popular service, at http://www.kagi.com.

139. *Successful Shareware*, *supra* note 137 ("'[C]rippleware': the program runs in semi-functional demo mode until the user pays up. He is then given a password of some kind that unlocks the product's full functionality. Or he may be sent a fully-functional version on disk or by e-mail, or be given access to an ftp site where the fully-functional version can be downloaded—but the basic idea is that the product is crippled until the user pays.").

carious liability for ISPs and workable copyright enforcement for individual copyright holders.

V. PROPOSAL

In order to effectively safeguard the rights of individual copyright holders, this Comment proposes a supplement to the DMCA's notice requirement. ISPs, OSPs, and individual copyright holders should be viewed as having different, but equally important, roles in reducing the crime of copyright infringement in the Internet neighborhood. Although this Proposal is designed for digital audio copyrights, it may apply to other forms of content as well. Instead of interest-group lobbying,[140] the legislative process, working within the normative framework of copyright law,[141] should have taken into consideration all of the stakeholders: Internet users, large industry associations and licensing collectives, ISPs, OSPs, software developers, *and independent copyright holders*. Although the DMCA apparently was not created by such a process,[142] this Proposal assumes that all of these stakeholder interests should be represented and balanced appropriately.

For the purposes of this Comment, discussions of OSPs will focus on the online services, rather than Internet access.[143] Since OSPs have greater control over both the user experience and the content, they are often in a better position to know exactly what their capabilities are and who comprises their user base.[144] Most importantly, OSPs

---

140. LITMAN, *supra* note 13, at 62.

> Perhaps a statute might be enacted over that stakeholder's pitched opposition; but efforts to accomplish that in the past have not succeeded. If the stakeholder will instead agree to accept the disadvantage in return for an advantage conceded by another stakeholder, there will be no pitched opposition and the bill will be much more likely to go through.

Id.

141. *Id.* at 79–80. "[T]he economic analysis of law . . . characterizes copyright as a system of incentives. Today, this is the standard economic model of copyright law, whereby copyright provides an economic incentive for the creation and distribution of original works of authorship." *Id.*

142. *Id.* at 144–145.

> There is no overarching vision of the public interest animating the Digital Millennium Copyright Act. None. Instead, what we have is what a variety of different private parties were able to extract from each other in the course of an incredibly complicated four-year multiparty negotiation. Unsurprisingly, they paid for that with a lot of rent-seeking at the expense of new upstart industries and the public at large.

Id.

143. However, as the Internet continues to grow and broadband access becomes more popular, the distinction between OSPs and ISPs may soon diminish or disappear because ISPs will probably choose to license increasing amounts of high-bandwidth content.

144. Although the recent news regarding Comcast's Web caching project, discussed earlier, reveals that the distinction between OSPs and ISPs might not be necessary because ISPs have the

are generally in managerial control over their domains and they maintain usage statistics, because doing so is often vital to their business.[145] Finally, and perhaps most importantly, OSPs receive an indirect benefit from copyright infringement because Internet users who are interested in unauthorized file sharing will patronize OSPs that enable this activity. ISPs may also receive a similar, albeit more attenuated, benefit.[146] Therefore, assisting with the policing of copyrights should be considered the cost of doing business for OSPs, and the initial steps to detect copyright infringement should be easier for individual copyright holders. Section A proposes a relaxed notice standard, and section B discusses the limited OSP duty, a single scan of publicly accessible domains, that the notice will trigger. Section C explains the responsive dialogue, following the OSP scan, between the OSP and the individual copyright holder. Following the dialogue, the individual copyright holder will provide a strict notice to the OSP, discussed in section D. Section E explains the necessary limitations required in order to prevent the OSP's duty from becoming unworkable.

A. A "Notice of Belief" Standard for Independent Copyright Holders

Instead of providing a pinpoint location of copyright infringement on the Internet, independent copyright holders should be able to make a good faith statement to an OSP[147] of their honest and reasonable belief that the intrinsic nature of the OSP's service makes the un-

---

ability to monitor their users (which results in net efficiency and performance benefits rather than taxing the resources of the ISP).

145. *See* Hitwise, *How We Do It*, *available at* http://www.hitwise.com/ss/howwedoit.html (last visited May 4, 2003) (stating that "Hitwise monitors Internet Service Provider (ISP) networks and other data sources to capture the usage patterns of the ISP's user base. Hitwise extracts from the partner ISP's networks a list of the websites visited and ranks them according to a range of industry standard metrics including page requests, visits and average visit length. Hitwise also extracts Click-Stream data analysing the movements of visitors between sites to provide subscribers with information on traffic to and from competitive sites.").

146. If some ISPs offer access to ports and services that facilitate or encourage the illegal sharing of files, this feature could be appealing enough that some users would make their ISP choices based on it alone.

147. Arguably, this portion of the Proposal could also apply to companies like Kazaa, an OSP that offers a network service in the form of software that enables a peer-to-peer file sharing capability. In addition, it could apply to ISPs because they have the ability to limit (and, at least in theory, track) the access through a specific port number. Port numbers, a subset of an Internet Protocol address, have been analogized to telephone extensions:

> A network port number functions similarly to a telephone extension. Taken together with a network address, a port number identifies both a computer and also a "channel" within that computer where network communication will take place. Just as different organizations may use the same extension numbers "inside" their primary phone number, different computers use the same set of port numbers.

Computer Networking, *What Is A Port Number?*, *available at* http://compnetworking.about.com/library/tips/blfaq012.htm (last visited Mar. 1, 2003).

authorized copying of their work more likely.[148] In addition, the copyright holder could provide a copy of each digital work and a keyword list to help the OSP locate instances of infringement. For some artists, the keyword list could merely be the artist's name and the title of the work. For others, more descriptive keywords might be necessary. Although most OSPs would likely have the necessary server space to temporarily store the copies submitted by the copyright holder, such storage (especially over a long-term period) would be unnecessary, because the purpose of the copy would be to help the OSP perform a single scan of its publicly accessible domains (as contrasted from any sort of on-going duty to continually scan for that work).[149] The OSP could discard the copy after performing the scan.[150] Once the OSP receives this information, the OSP would have a limited duty to perform a single scan of only those domains or ports that are free and open to the public.

Changing this aspect of the notice requirement would create a more efficient search process, analogous to most methods of searching. When an Internet user performs a search on an Internet search engine, she enters a series of terms that will result in the most accurate return of links. However, given the vast number of Web pages and services on the Internet, she will likely err on the side of receiving too many return links in order to minimize the risk of excluding a good link. This is a good strategy for finding an online resource, but the notice requirement eschews a wide-to-narrow scheme, requiring a single pinpoint location of infringement in the notice that a copyright holder must give to an ISP. Although the current structure of the notice requirement reflects a policy choice of placing the total burden on the copyright holder as the primary beneficiary of the right, it is likely predicated on the following assumptions: (1) there are adequate search tools available to copyright holders to detect infringement; (2) anti-circumvention technology will adequately prevent or reduce unauthorized file sharing; (3) the location of infringement will always be static or last long enough to send compliant notice; and (4) the copyright holder will be able to communicate that location (either in the form of an IP address or whatever proprietary information the OSP uses) ade-

148. Note that this alteration of the notice requirement should not remove the ISP from the protection of any applicable safe harbor provisions. Given the nature of the later proposed error correction between ISP and the individual copyright holder, any knowledge of infringement should not be considered evidence of actual or constructive knowledge of infringement. If it were otherwise, the ISP or OSP would be creating a basis for its own liability.

149. Further, this aspect of the Proposal is likely to be no more cumbersome than the processes involving ISP and subpoenas to identify infringers in 17 U.S.C. § 512(h)(5).

150. Although the OSP would certainly want to maintain records of the interaction for its own records, keeping the actual copy should not be necessary.

quately to the ISP in a clear and timely manner. These are not necessarily safe assumptions to make.

As previously stated, Web search engines are generally restricted to searching via HTTP, with some exceptions.[151] This means that FTP searches and dynamic HTTP services[152] will not be searchable by Internet users; therefore, the first assumption fails. Further, P2P networks exist separate from the Internet, and their popularity indicates that more piracy is taking place here, rather than on the Web. In addition, anti-circumvention methods frequently found themselves cracked open by diligent hackers who distribute the keys on the Internet anonymously.[153] Therefore, anti-circumvention methods may supplement, but not supplant, a copyright holder's plan to substantially reduce unauthorized file sharing on the Internet. The third assumption fails because it does not take into account the prominence of dynamic Internet Protocol addresses[154] or firewalls. Finally, as the earlier discussion of *Hendrickson* illustrates, proprietary locator information, such as eBay auction numbers, can prove to be a stumbling

---

151. Even MP3.Lycos.com is confined to searches via HTTP, although Internet users may shares files directly from their hard drives via HTTP. FTP shares will also appear in search results. *See* MP3.Lycos.com, *available at* http://mp3.lycos.com (last visited Feb. 16, 2002).

152. That is, services that change based on input from the administrator or other users and whose Web address is altered periodically.

153. Michelle Delio, *The Key to Encryption*, *available at* http://www.wired.com/news/ebiz/0,1272,44740,FF.html (last visited Feb. 17, 2002); Michelle Delio, *Hackers Win Security Challenge*, *available at* http://www.wired.com/news/technology/0,1282,43234,00.html (last visited Feb. 17, 2002); Paul Boutin, *Philips Burning on Protection*, *available at* http://www.wired.com/news/politics/0,1283,50101,00.html (last visited Feb. 17, 2002).

> If such a law were passed, it's unlikely the proposed standard would be as simple as adding errors to the aging Red Book format. "My understanding of the current protection schemes is they're very easy to defeat," Doris says. "If there are millions of CDs out there, there'll be lots of code posted to the Net—whether it's legal or not."

Id. In May 2002, Sony attempted to roll out a new form of copy protection for compact discs that would prevent a user from being able to copy the audio tracks onto a computer, but this method was easily circumvented: "After an initial attempt to play the disc on a PC resulted in failure, the edge of the shiny side of the disc was blackened out with a felt tip marker. The second attempt with the marked-up CD played and copied to the hard drive without a hitch." Wired News, *CD Crack: Magic Marker Indeed*, *available at* http://www.wired.com/news/technology/0,1282,52665,00.html (last visited Apr. 6, 2003). Not only was the copy protection scheme easy to defeat, but it reportedly damaged Macintosh computers, causing them to crash. *Id.*

154. IPInfo, *available at* http://www.lawrencegoetz.com/programs/ipinfo/ (last visited Feb. 17, 2002).

> A little bit about your IP address (Internet Protocol address). When you connect to the internet, either via your internet service provider (AOL, Prodigy, etc.), or your office LAN connection, you are assigned an IP address. This address identifies your computer from the other computers on the internet. Your IP address can be either static, meaning it never changes, or dynamic, meaning each time you dial-in or login you are assigned a new address for that session.

Id.

block to efficiently providing notice to an OSP.[155] Without being able to rely on these assumptions, the apparent efficacy of the DMCA's notice requirement breaks down, at least for independent copyright holders. To counter this failure, the proposed notice of belief is a cooperative search process that allows for better feedback and error correction. By providing copies and filenames of works suspected to be the subject of unauthorized copying, the copyright holder is able to control the "search terms" of the detection process, and the OSP appropriately functions as the engine because it is in a better position to know its domain and run a reasonable scan.

B. A Reasonable Scan by OSPs

Having received the filename, a copy of the digital work, and a keyword list, the notified OSP would be required to run a scan of only those publicly accessible domains[156] or IP addresses, comparing the information to those files being served. This could be accomplished in a number of different ways, depending on the nature and size of their service. Similarly, the need to run multiple scans would likely depend on the size of the OSP's domain. For instance, in the event that the OSP incorporated multiple protocols like FTP, HTTP, and Gnutella, then a separate scan across each protocol might be necessary. If the OSP did not already monitor usage statistics, server backups, and file transfers, a number of technologies already exist to fulfill this function.[157] Indeed, technology similar to that discussed in *Napster* could be reformed to search for unauthorized copies.[158] In addition, royalty management software could be leveraged here. However, the use of such software would not create a guarantee against unauthorized file sharing, and copyright holders would still require the assistance of the DMCA in order to reduce copyright infringement on the Internet. Although one might argue that the absence of such software in great quantity is evidence of its inability to function in the modern Internet, such an argument rings hollow considering that there are no legal or economic incentives for this software to be created. There is no de-

155. *Hendrickson*, 165 F. Supp. 2d at 1090–92.

156. The word "domain" does not refer to the geographic reach of the services; after all, online services are, by their very nature, global. Instead, this refers to the range of services provided and the Internet protocols used by those services.

157. For example, see http://www.copyrightnet.com. This website provides digital rights management and tracking software.

158. JESSICA LITMAN, DIGITAL COPYRIGHT 25 (2001). "The Internet sometimes gets characterizes as a giant copying machine that facilitates widespread and undetectable copyright infringement. That's about 50 percent hype—the Internet facilitates widespread copying, but it also facilitates detection of copying." *Id.*

mand for it currently, because no service provider has any legal obligation to buy and use it. Given the numerous types of searching tools available to OSPs, this single scan requirement could fairly, efficiently, and appropriately balance the burdens of detecting copyright infringement between copyright holders and OSPs.

C. A Responsive Dialogue

Continuing the spirit of neighbor-like cooperation between copyright holders and OSPs, a responsive dialog would allow for error correction presently absent from the notice requirement of the DMCA. After performing a scan using reasonable efforts to detect the complained of works, the OSP would submit a list of hits, including Internet Protocol numbers[159] or an equivalent[160] back to the copyright holder, who would then visit these pinpointed locations and confirm whether the discovered material was infringing or not.[161] The copyright holder would notify the OSP which of the files were matches, and the OSP would not take additional action until it received confirmation from the copyright holder.[162] In the alternative, if the found files matched the copyright holder's submission perfectly, then the OSP could initiate the takedown procedure on its own or send identifying user information, as described in the DMCA.[163] This Proposal does not change the safe harbor protection offered by the DMCA to ISPs, and the proposed OSP sub-category would retain the same protection.[164] Although this step would reduce the speed of responding to copyright infringement, it would perform the important function of reducing potentially mistaken takedowns.

---

159. Internet Protocol numbers are Internet addresses that would enable an examination of the content being served to the world.

160. In order for the individual copyright holder to view and verify the allegedly infringing material.

161. This aspect of the Proposal would not affect 17 U.S.C. § 512(h), because the information given to the copyright holder here is not an identification of the infringer but rather the infringement itself.

162. However, if the OSP otherwise had knowledge of infringement, then it would be required to perform a take-down.

163. 17 U.S.C. § 512(c). ISPs are immune from liability resulting from a take down of legally owned material if the ISP returns the material within ten days of receiving notice that such material was owned by the user.

164. Since this Comment does not propose a change to the safe harbor protection itself, OSPs would remain immune from the liability for the unknown activities of users, as well as from wrongful takedowns.

D. A Notice of Infringement

If the copyright holder determined that the presence of the work was infringing, the copyright holder would then submit formally compliant notice[165] to the OSP, and the OSP would initiate the takedown procedure[166] described in the DMCA. The copyright holder could easily provide formal notice in light of the information shared between the copyright holder and the OSP. The factors would not need to be changed from those enumerated in 17 U.S.C. section 512(c).

E. Limitations

Certainly, this Proposal poses potential for abuse by large organizations that own the copyrights in thousands of works. In a flurry of correspondence, an organization like the RIAA could flood a small OSP with "Notices of Belief" and the OSP might not be able to respond adequately. Therefore, the proposed mechanism should be limited to individual copyright holders. The existing notice requirement would remain to serve organizations or associations of copyright holders.

In addition, this Proposal should not be understood to create an affirmative duty on the part of OSPs to clear their domains of copyright infringement. Nor should it be construed as an opportunity for copyright holders to be free of the burden to locate infringement, because the proposed system requires that both OSPs and copyright holders work together to reduce unauthorized file sharing: copyright holders must submit the initial search terms, OSPs must perform a single scan, and copyright holders must then confirm the infringement. Therefore, the Proposal would not result in an unworkable amount of submissions.

In addition, OSPs must not be saddled with an ongoing duty to continually scan their publicly accessible domains for the complained of files. After all, to do so would convert this Proposal from a cooperative framework to a singular affirmative duty carried by OSPs. Although this problem might be alternatively solved by a reduction in the duration of exclusive rights under copyright for music, such a proposal is outside the scope of this Comment.[167] Absent such a change

---

165. Because of the lowered level of involvement on the part of the copyright holder, the "substantially compliant" standard could be raised—that the copyright holder's notice comply strictly with each factor.

166. 17 U.S.C. § 512(c)(1)(C).

167. For a captivating discussion of the Sonny Bono Copyright Term Extension Act, see J. Michael Keyes, *Whatever Happens to Works Deferred?: Reflections on the Ill-Given Deferments of the Copyright Term Extension Act*, 26 SEATTLE U. L. REV. 97 (2002).

in copyright protection, this Proposal would need to include a provision at which time the OSP would wash its hands of the duty to scan and then dispose of the digital copies submitted by the copyright holder.

VI. COOPERATION: A NEIGHBORHOOD NORM FOR THE INTERNET

A. Neighborhood Watch

As neighbors on the information superhighway, individual copyright holders and ISPs each have a stake in the health of the Internet and in the variety of its content. Although some copyright owners have pursued claims against individual users for copyright infringement,[168] such persons represent a distinct minority because such pursuit, to say nothing of the cost of litigation, is expensive and will likely reduce their popularity with patrons.[169] Professor Ginsburg suggested that "authors and copyright owners may be able to work with commercial online services to control the gate between the author and the public."[170] However, this statement was made before the advent of Napster, Kazaa, and similar services; as stated earlier, files can now be globally shared via the World Wide Web without any need to negotiate through the contractual access schemes created by an OSP.[171]

Professor Ginsburg also suggested that copyright holders could band together in an artistic rights collective responsible for licensing as well as policing functions.[172] Although this idea has some merit, such collectives do not satisfy the needs of all copyright holders because they require artists to give up control over copy permissions, which they may be reluctant to do.[173] Although cooperation between individual copyright holders and ISPs is probably the most efficient compromise, some might argue that the government, as a stakeholder, should play a stronger role.

---

168. Tussey, *supra* note 1, at 1133.

169. Ginsburg, *supra* note 37, at 1488.

170. *Id.*

171. *See* Gnutella.com, *What is Gnutella?*, *available at* http://www.gnutella.com/news/4210 (last visited Feb. 6, 2002) ("[The Gnutella client] creates a revamped atmosphere on the Internet, enabling users to share information like never before. To put it simply, Gnutella puts the personal interaction back into the Internet. When you run Gnutella software and connect to the Gnutella Network, you bring with you the information you wanted to make public. And you choose what information to share. You can choose to share nothing; you can choose to share one file, a directory, or your entire hard drive.").

172. Ginsburg, *supra* note 37, at 1489.

173. *Id.*

B. The Limited Role of Government: Legislation and the Judicial Process

The role of government in identifying and locating copyright infringement on the Internet should not extend past creating law with legislation and enforcing that law through the judicial system. The creation of an administrative agency to detect copyright infringement on the Internet would likely be impractical. Because of the distributed nature of the Internet and the diverging, even proprietary, quality of online services, any active regulation of the Internet requires more than a single entity.[174] The time involved in learning the systems and networks of every OSP whose service increased the likelihood of copyright infringement would be an insurmountable cost, precluding any meaningful regulation and enforcement. Further, there would undoubtedly be a perception that privacy rights would be implicated by the nature of the government's presence. In reality, however, there would be no privacy violation because the Proposal limits scans to publicly available domains or publicly available user information. Internet users could guarantee that their personal files would not so much as be glanced at by an OSP if the user was able to password-protect directory access (a common feature on many Internet hard drive services). Scanning domains should be the responsibility of OSPs, not the government, and not because they can perform the scans, but because some of them are doing so currently.

Comcast, an ISP, recently made headlines for an activity that was previously believed to be achievable only by the Federal Bureau of Investigation's "Echelon/Carnivore"[175] technology: tracking and cataloging Web usage.[176] Comcast accomplished what was previously thought to be an impossible challenge to ISPs in order to save money and improve the performance of its cable Internet service.[177] In its caching system, Comcast recorded the Internet Protocol address of its subscribers, the Internet address of the Web pages requested, and the actual content of the most popular pages in its automatically activated proxy servers; America Online (AOL) was reported as using a similar system to increase performance.[178] While such technology raises sig-

174. Interestingly, the DMCA can be viewed as forward looking in that it created a distributed means for scanning a distributed network.

175. Declan McCullagh, *Senate Oks FBI Net Spying, available at* http://www.wired.com/news/politics/0,1283,46852,00.html (last visited Feb. 17, 2002).

176. Stefanie Olsen & Rachel Konrad, *Comcast Privacy Move Its Latest Woe, available at* http://news.com.com/2100-1023-836937.html (last visited May 4, 2003).

177. *Id.*

178. *Id.*

nificant privacy concerns[179] (indeed, many have commented that the caching invites the interest of law enforcement officers and civil action litigants[180]), Comcast and AOL's newly discovered ability puts to rest the foolish contention that it was impossible for ISPs to monitor Internet activity.[181] Given the ability of OSPs to scan their domains, it seems clear that copyright holders should not shoulder the initial burden of detection alone.

C. Support for Independent Copyright Holders

The present burden on copyright holders, especially individuals not represented by a recording collective, is overwhelming because they are unable to efficiently find instances of infringement, in part because there is no guarantee that they are sufficiently familiar with the mechanics of the Internet. The real problem for copyright holders *qua* enforcement agents is that they are likely unable to learn the intricacies of the numerous OSP domains that exist on the Internet. Thus, they are unable to complete the basic tasks of identifying and locating infringement. Any regime that exists to further the creative endeavors of artists should maximize the amount of time artists spend creating so that society receives a continuous and robust stream of new art.

The problem of P2P technology has been particularly vexing to the RIAA, and it has attempted to reduce copyright infringement through litigation[182] and other means. Wired Magazine recently listed the following twelve tactics: gluing review compact discs (CDs) inside portable stereos; sending out promotional analog cassettes (in lieu of distributing digital CDs); employing digital watermarks on CDs; dis-

---

179. Stefanie Olsen & Rachel Konrad, ZDNet News, *Privacy Fears Stoke Ire Against Comcast*, *available at* http://zdnet.com.com/2100-1105-837029.html (last visited Feb. 15, 2002) ("'This information has never been connected to individual subscribers and has been purged automatically to protect subscriber privacy,' Burke said. 'Beginning immediately, we will stop storing this individual customer information in order to completely reassure our customers that the privacy of their information is secure.'").

180. *Id.*

181. Olsen & Konrad, *supra* note 176.

182. Katie Dean, *RIAA Hits Students Where It Hurts*, *available at* http://www.wired.com/news/digiwood/0,1412,58351,00.html (last visited Apr. 6, 2003).

> The Recording Industry Association of America apparently took a page from the military handbooks of coalition forces in Iraq this week when it attempted to 'shock and awe' college music pirates by hitting them with hefty lawsuits.
>
> The trade group is suing four students for operating Napster-like file-sharing services on their campus networks.

Id. Interestingly, the RIAA chose this public action instead of proceeding with the takedown process set forth in the DMCA. *Id.* Arguably, this decision implies the inadequacy of a private DMCA takedown—such private actions are unlikely to shape Internet norms, whereas publicized litigation of college students may have profound effects (one of which may be to diminish further the RIAA's image).

tributing bogus audio files, disguised as real songs, on P2P networks; hiring many people to stand in line on P2P servers so as to prevent others from accessing the files; placing copy protection on CDs; selling digital music files at competitive prices online; hosting pre-release listening parties; allowing those who purchase CDs to access additional music or video files when their CD is inserted in a computer; suing the networks or software companies themselves, rather than the individual users; lobbying Congress for stronger copyright sanctions or the ability to hack into P2P users' hard drives; and running advertising campaigns, hoping to change Internet norms.[183]

Of these numerous tactics, few are practicable for independent copyright holders because they require substantial financial resources. For instance, it is unlikely that many independent copyright holders are able to pay for lobbying efforts of protracted litigation against software companies like Kazaa. Further, independent musicians are not likely willing to sacrifice their reputation by engaging in guerilla copyright protection tactics, since such a maneuver would place their small fan base at risk.

Recent developments in the digital rights management and Internet service provider industries indicate that the burden on copyright holders increased considerably after the recent American recession of 2001 and that the challenge of tracking Internet usage is not as difficult for ISPs and OSPs as it once seemed. Since July 2001, a number of content protection companies have shut down or laid off significant portions of their staff.[184] This phenomenon is due not only to the recession, but can also be attributed to inherent problems in the technology used to protect digital works.[185] Because safeguarding such content usually involves completing multiple-step purchases, navigating through password dialogs, and dealing with proprietary encryption systems, application of these controls to new markets like electronic books has created significant roadblocks to adoption.[186] Further, because of concerns about unauthorized copying, such protections schemes prevent or hamper the portability of the protected work (and ease of portability is arguably the most important aspect of a digital work).[187] The scant remaining players in the digital rights manage-

183. Matt Bai, *Hating Hilary*, WIRED MAGAZINE, Feb. 2003, at 98.

184. Wade Roush, *The Death of Digital Rights Management?*, *available at* http://www.techreview.com/articles/innovation10302.asp (last visited Feb. 16, 2002).

185. *Id.*

186. *Id.*

187. *Id.*

ment industry provide few practical assurances to today's digital content creators.[188]

Although some may argue that cases like *ALS Scan* demonstrate the success of the DMCA as it relates to copyright holders' ability to find infringing use on the Internet, supply adequate notice to the OSP, and have the material taken down, *Hendrickson v. eBay*[189] highlights the problem inherent in the notice mechanism when the copyright holder is a person, rather than a large business or licensing collective; creative individuals that are unaffiliated with a licensing collective do not likely have the resources to spend hunting down infringement.

While it may seem easy to discover infringing activity on the Internet, publicly available search engines access only a small percentage of the Internet. Indeed, many commercial search engines are compromised by contracts that predetermine the ordering of results.[190] Many businesses pay money in order to be listed when certain search terms are entered.[191] Further, even Web sites that do not pay fees for search engine placement place metatags in HTML code in order to appear before others.[192] Although such Web sites arguably make it easier to determine the nature of their service, it nevertheless obscures search engine results, and more importantly, reduces the control that copyright holders have in their endeavors to end infringement of their works on the Internet. Not only do search engines fail to scan all pages on the Web,[193] but existing search engines are often limited to scanning HTTP documents, which do not include FTP servers, Gnutella servers, or the Kazaa network.[194] Usenet newsgroups, FTP servers, and publicly available Internet hard drives are all unavailable to search engines without software that is specifically created to scan those domains. Thus, copyright holders who wish to prevent unauthorized copying and distribution of their works on the Internet must spend considerable amounts of time manually paging through publicly available domains on the Internet to quell the flow of infringement. Cooperation, therefore, is an imperative.

188. *Id.*

189. 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

190. Rik Fairlie, *Search Engines Rank Revenue Over Relevance*, *available at* http://computers.cnet.com/hardware/0-1016-8-20886940-1.html (last visited May 4, 2003).

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

D. The Hybridized Enforcing Authority: Independent Copyright Holders and OSPs

In *Napster*, the court made the following statement:

> Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. Napster has both the ability to use its search function to identify infringing musical recordings and the right to bar participation of users who engage in the transmission of infringing files.[195]

Although it is unclear what authority the court was referencing in this statement, it clearly expresses the sentiment that OSPs have a responsibility to use their best efforts as citizens of a lawful Internet. OSPs, however, cannot read the minds of copyright holders, and as such, it is impossible for an OSP to know which files are shared with the permission of the copyright holder and which are infringing uses by an end user. Therefore, because OSPs are not in the best position to identify instances of infringement, they cannot shoulder the burden of an affirmative duty to police their domains. However, OSPs should share in the responsibility for enforcing copyright law because they derive a substantial benefit, albeit indirect, from the infringing activity of their users, as is illustrated in the example below.

If an OSP derives a benefit from unauthorized file sharing, then, arguably, the OSP should bear part of the cost to the copyright holder.[196] Imagine that there is a business called FullOnFiles.com that provides an Internet hard drive service allowing users to upload and share diverse types of data. If FullOnFiles.com becomes a well-known service, at least part of that reputation will be built on the actual services it offers, distinguished from its overt marketing.[197] At least some of the users of FullOnFiles.com will share files in derogation of copyright owners' exclusive rights, and this use, like others, could quickly become part of the FullOnFiles.com reputation. If this

---

195. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001).

196. CNN.com, *Anti-Smoking Groups Urge Cigarette Tax Hikes*, *available at* http://www.cnn.com/2002/US/02/26/cigarette.tax.increase/index.html (last visited Mar. 5, 2002). Tobacco taxes exist not only to reduce the number of cigarettes sold, but they also function, at least in theory, to defray the societal cost from tobacco-related illnesses. A similar scheme, closer to copyright issues, exists in some countries regarding the sale of blank recordable compact discs (CD-R). For each CD-R sold, a small percentage of the sale goes to recording industry concerns. Although this is not necessarily done to discourage the consumption of CD-Rs, the amount collected by the recording industry theoretically compensates those artists whose music is copied.

197. For instance, if FullOnFiles.com allows a capability that allows users to browse each other's Internet hard drives, then this capability would likely be a significant incentive for members to use FullOnFiles.com rather than other services which do not provide this.

kind of infringing use was popular, then FullOnFiles.com would derive a benefit by virtue of the infringing activity. If this benefit is substantial enough to affect in any way the nature of FullOnFiles.com's business or marketing plans, then it should carry some of the responsibility for routing out infringement on the Internet. In contrast, such a benefit is not realized by an ISP that provides mere Internet access because its reputation will be built on price points, bandwidth, and reliability.

OSPs whose business is a lawful enterprise would not be unduly burdened by this Proposal, because many such businesses already possess the necessary tools to run ad hoc scans of their domains.[198] Since the Proposal does not create an ongoing duty to monitor networks, few additional resources would be necessary. After all, OSPs are already required by the DMCA to respond to notification of infringement by copyright owners,[199] and this Proposal would not significantly change the nature of this required resource.

Copyright owners are in the best position to know whether their work is being shared, precisely because such sharing is usually at the copyright owner's discretion, and also because digital works do not necessarily include embedded copyright information. However, as discussed above, copyright owners are not often learned in the intricacies of every OSP whose service may be apt to create or encourage instances of infringement of their work by end users. Thus, their abilities, the copyright owner's ability to identify and the OSP's ability to locate, should be combined to maintain a responsible and lawful Internet.

E. Allocating Burdens, Considering Privacy, and Clarifying Fair Use

To be sure, copyright "was designed to be full of holes,"[200] placing a greater importance on the sharing of works than on the incentives for creators, but the current iteration of the DMCA, as it relates to the reduction of copyright infringement on the Internet, is woefully inadequate because it fails to establish a meaningful enforcing authority. While the current construction reflects a general policy consideration that the Internet should be unfettered by restrictions, the implementation of this policy was short-sighted. Copyright holders are arguably in the best position to identify the infringement of their

198. Olsen & Konrad, *supra* note 176.

199. Presently, in order to comply with the DMCA, ISPs likely need both technology and personnel who are able to locate files and initiate take-downs; therefore, adopting this Proposal, widening only the scope of the initial scan, would not likely impact the ability of OSPs to comply.

200. LITMAN, *supra* note 13, at 79.

rights, but ISPs are in the best position to locate the files because they control their domains and Internet Protocol addresses more directly.

Some Internet users may balk at the notion that their OSP might scan their activities, but such privacy concerns fail to recognize the limited nature of this Proposal. After all, OSPs would only scan *publicly available* domains. If a user was concerned about such a scan, the mere use of password protection would take the domain out of the scope of the OSP scan. Additionally, the relationship between OSP and user is governed by contract law, providing adequate notice to the user of the OSP's policy.[201]

While the doctrine of fair use,[202] which corrects market failures that are due to impossibly high transaction costs, is a defense to an infringement action, it does not apply where an individual shares, without authorization, copyright-protected works with the world via the Internet.[203] Factors to be considered when determining whether a use

---

201. For example, AT&T Broadband cuts a much wider swath in its subscriber agreement, below, than does the Proposal:

> (g.) Monitoring of Postings and Transmissions. AT&T Broadband shall have no obligation to monitor postings or transmissions made in connection with the Service. However, Customer acknowledges and agrees that AT&T Broadband and its agents shall have the right to monitor any such postings and transmissions, including without limitation e-mail, newsgroups, chat, IP audio and video, and web space content, from time to time and to disclose them in accordance with Section 4 of this Agreement, and as otherwise required by law or government request. AT&T Broadband reserves the right to refuse to upload, post, publish, transmit or store any information or materials, in whole or in part, that, in its sole discretion, is unacceptable, undesirable or in violation of this Agreement.
>
> (h.) Eavesdropping. AT&T Broadband's facilities are used by numerous persons or entities including, without limitation, other subscribers to the Service. As a result, there is a risk that Customer could be subject to "eavesdropping." This means that other persons or entities may be able to access and/or monitor Customer's use of the Service. This risk of eavesdropping exists not only with AT&T Broadband's facilities, but also on the Internet and other services to which access is provided as a part of the Service. Any sensitive or confidential information posted, stored, transmitted or disseminated by Customer is done so at Customer's sole risk, and neither AT&T Broadband nor its affiliates shall have any liability whatsoever for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to such actions by Customer. Customer acknowledges that software programs claiming to be capable of encryption are commercially available. AT&T Broadband makes no representation or warranty regarding the effectiveness of such programs.

AT&T Broadband, *AT&T Broadband Subscriber Agreement*, *available at* http://help.broadband.att.com/faq.jsp?content_id=973&lobid=1 (last visited Apr. 6, 2003). *See also* discussion, *supra* Part VI.B.

202. 17 U.S.C. § 107 (2000); *see, e.g.*, Matthew D. Bunker, *Eroding Fair Use: The "Transformative" Use Doctrine after Campbell*, 7 COMM. L. & POL'Y 1 (2002) (discussing the development of the fair use doctrine).

203. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015–17 (9th Cir. 2001).

is a fair use include the purpose and character of the use,[204] the nature of the given work,[205] the portion of the work used,[206] and the effect of the use on the value of the work or the potential market for the work.[207] After the *A&M Records v. Napster* decision,[208] however, the free and open public distribution of digital music to the world constituted infringement of the copyright holder's right to publicly perform the work, to distribute copies, and to perform the work publicly by means of a digital audio transmission,[209] and the court determined that such use was not fair use. By prohibiting unauthorized file sharing via the Web, this decision preserves the limited monopoly right granted by American copyright law, ensures that the Audio Compact Disc market will remain,[210] and safeguards the ability of artists to enter the digital music delivery market as it develops.

VII. CONCLUSION

The Internet has been described as an information superhighway, a cyberspace, and a global village, but the DMCA fails to support these metaphors, least of all the global village or neighborhood. Instead of privatizing copyright enforcement and placing all of its burdens on the individual copyright holder, the notice requirement DMCA should be supplemented for independent copyright holders so as to reflect the Neighborhood Watch model, thereby strengthening modern copyright norms.

Although the DMCA responded to significant inadequacies of traditional copyright law in relation to the Internet, it needs revision. The DMCA's notice requirement appears predicated on unreliable assumptions about the nature of the Internet and, alone, copyright holders *qua* initial enforcing authorities are unequipped to meet the challenge of finding unauthorized file sharing on the Internet. Moreover,

---

204. 17 U.S.C. § 107 (2000). This includes an inquiry as to whether the use is commercial or educational in nature.

205. *Id.*

206. *Id.*

207. *Id.*

208. 239 F.3d at 1011–13 (interestingly, this decision marks the first holding that specifically restricts the Internet-only action of global file sharing of copyrighted works as illegal—other holdings have had real world equivalents).

209. *Id.* at 1013–16.

210. *Id.* at 1018, 1026 (affirming the finding of the lower court that "both the market for audio CDs and market for online distribution are adversely affected by Napster's service. . .the court did not abuse its discretion when it found that, overall, Napster has an adverse impact on the audio CD and digital download markets."; also holding that destruction of Napster, Inc. due to an injunction was speculative "compared to the statistical evidence of massive, unauthorized downloading and uploading of plaintiffs' copyrighted works—as many as 10,000 files per second by defendant's own admission.").

copyright law was never intended to transform artists into police. Although allocating the totality of the burden to copyright holders may be satisfying in the abstract, it fails in reality. Unfortunately, the government is not likely able to effectively police the Internet for copyright infringement. Instead, OSPs and copyright holders should be encouraged by a revision to the notice requirement of the DMCA to work together to significantly reduce infringement on the Internet. Copyright holders are in the best position to identify their works, and OSPs are in the best position to locate them once they receive adequate information from copyright holders. Indeed, this is an efficient, effective, and cooperative way to reinforce copyright norms on the P2P- and Web-based neighborhoods of the Internet.