WHOM THE GODS WOULD DESTROY: WHY CONGRESS PRIORITIZED COPYRIGHT PROTECTION OVER INTERNET PRIVACY IN PASSING THE DIGITAL MILLENNIUM COPYRIGHT ACT

*Lateef Mtima**

The problem of illegal file-sharing and related acts of Internet infringement is one of the most important copyright challenges of the day. Not only does such activity threaten the property interests of copyright owners, but given the attendant prospect of vicarious copyright infringement liability that confronts Internet Service Providers (ISPs), this conduct also threatens the vitality of the Internet as a whole. In 1998, Congress undertook to address this issue by passing the Online Copyright Infringement Liability Limitation Act, Title II of the Digital Millennium Copyright Act (Liability Limitation Act). The principal purpose of the Liability Limitation Act is to remove ISPs from the copyright infringement litigation battles which inexorably arise between copyright owners and unauthorized file-sharers of their works. Under the Liability Limitation Act, so long as an ISP conducts its service in accordance with the Act's requirements, which include removing infringing material from the Internet and disclosing the identities of suspected unauthorized file-sharers and other infringers, the ISP is essentially immune from vicarious liability claims. Some recent court decisions interpreting the Liability Limitation Act, however, threaten this pragmatic balance of the pertinent Internet constituent interests. At least two federal circuits have construed a purported ambiguity in the language of the Act, so as to hold that certain kinds of ISPs are not required to disclose the identities of suspected infringers in response to subpoenas issued under the Act. Under these holdings, copyright holders are instead required to involve ISPs in copyright litigation and discovery, solely to obtain the identities of suspected infringers.

---

* © 2009, Professor of Law and Founder/Director of the Institute of Intellectual Property and Social Justice, Howard University School of Law. I would like to thank Robert Cumbow and Laurence Nolan, for their extremely helpful comments on various drafts of this article. I would also like to thank Tiffany Tucker, HUSL '09, Ritu Narula, HUSL '10, and Izukanne Emeagwali, HUSL '10 for their excellent research assistance. Finally, I would like to thank Dean Kurt L. Schmoke for research support. Any errors are my own.

This Article proposes that these court decisions misconstrue the terms of the Liability Limitation Act, and contravene the express objectives of the statute. This misconstruction of the Act needlessly entangles ISPs in infringement disputes in which they have no immediate stake, and further, does little to enhance legitimate Internet user privacy interests, because it affords ISP subscribers no greater legal protection than already provided under the law. Moreover, by impeding infringer identity disclosure, this judicial course not only increases the costs involved in the inevitable disclosure of infringer "cyber-pseudonym" identities, it also facilitates socially undesirable and morally debilitating conduct, ultimately burdening the Internet community as a whole. Accordingly, future courts should reject these rulings, and construe the Liability Limitation Act to require all ISPs to disclose subscriber identities in response to subpoenas issued thereunder. This would preserve the proper balance between copyright holder property rights and Internet user privacy interests, and further, impose the responsibility for preventing or redressing Internet infringement where Congress intended: on copyright holders and infringing Internet users, and not on ISPs and the overall Internet community.

INTRODUCTION

The problem of illegal file sharing and similar acts of copyright infringement on the Internet is one of the most familiar legal controversies of our time. Each day, thousands of unauthorized copies of copyrighted works are distributed on the Internet. Moreover, the attendant social issues are often far from black and white. While many acts of unauthorized file sharing are no more than base piracy, not all of this conduct can be fairly characterized as such. Some unauthorized file sharing occurs in naïve ignorance of the copyright legal regime. In other instances, such conduct might be undertaken by copyright end-users as a means of protest against the leading entertainment conglomerates. These end-users believe that the major corporate copyright holders are engaged in a system of monopolistic price gouging of the public, and that widespread distribution of the copyrighted material that these entities control serves the spirit, if not the letter, of the copyright law.

Whatever one's view of the relevant social debates, however, some facts are plain. On the one hand, unauthorized Internet distribution of copyrighted works is a prima facie violation of the rights of copyright holders.[1] At the same time, the Internet has otherwise evolved into a legitimate—and arguably indispensable—means of communication and education, as well as a vital source of news and information in modern society. Consequently, it is essential

1. *See, e.g.*, Advance Magazine Publishers, Inc. v. Leach, 466 F. Supp. 2d 628, 637 (D. Md. 2006).

to avoid the curtailing of Internet use and access as a solution to the problem of Internet copyright infringement. Ubiquitous Internet access benefits everyone, and it would be to society's overall detriment if such access were to be unduly restricted or hampered in the cause of protecting the property rights of intellectual property owners.

A. The Online Copyright Infringement Liability Limitation Act

In 1998, Congress undertook to address this dilemma by passing the Online Copyright Infringement Liability Limitation Act Title II of the Digital Millennium Copyright Act (the Liability Limitation Act).[2] The principal purpose of the Liability Limitation Act is to remove the Internet, or perhaps more specifically ISPs, from the center of the battle between copyright holders, unauthorized file-sharers, and other Internet copyright infringers.[3] Under traditional copyright jurisprudence, third parties can be held vicariously liable for the copyright misconduct of others, such as when the owner of a Xerox machine knowingly permits it to be used by a third party to make unauthorized copies of a copyrighted work.[4] In the same vein, an ISP could be held liable for the infringement acts of unauthorized file-sharers who obtain their access to the Internet through the ISP.[5] If copyright holders are able to recover from ISPs for the misconduct of their subscribers, however, ISPs will likely take a more restrictive approach in deciding to whom they will provide Internet service and on what terms such service would be provided. In short, widespread Internet access could be sacrificed in the cause of protecting copyright property rights.

The Liability Limitation Act avoids this undesirable result by providing certain "safe harbor" provisions that shield all ISPs from vicarious liability claims arising from the copyright infringement activities of their subscribers and other individuals.[6] In essence, when a copyright holder notifies an ISP of alleged infringement activity, so long as the ISP adheres to the requirements of the Act, such as removing the infringing material from the Internet or expeditiously disclosing the identities of the suspected infringers to the complaining copyright holder, the ISP is effectively immunized

---

2. 17 U.S.C. § 512 (2006).

3. *See id.*

4. *See, e.g.*, Metro-Goldwyn-Mayer, Inc. v. Grokster Ltd., 380 F.3d 1154, 1164 (9th Cir. 2004) ("Three elements are required to prove a defendant vicariously liable for copyright infringement: (1) direct infringement by a primary party, (2) a direct financial benefit to the defendant, and (3) the right and ability to supervise the infringers.").

5. *See, e.g.*, *Advance Magazine Publishers*, 466 F. Supp. 2d at 637.

6. § 512(a)-(e), (g), (i).

from vicarious liability for the infringement misconduct.[7] As a result, ISPs need not restrict Internet service as a means by which to decrease their vicarious liability exposure, and widespread Internet access need not become hostage to the cause of copyright protection.

B. Judicial Disruption of the Balance Achieved by the Liability Limitation Act

For some time now, the Liability Limitation Act has embodied a workable compromise between the pertinent interests of ISPs and the competing interests of copyright holders and Internet copyright end-users.[8] Rather than burden ISPs (and ultimately, legitimate Internet copyright end-users as well) with the responsibility and cost of preventing surreptitious Internet infringement, the Act allows ISPs simply to point complaining copyright holders in the direction of the alleged infringer subscribers, and then exit from the ensuing skirmish.[9]

Some recent judicial interpretations of the Liability Limitation Act, however, undermine this pragmatic balance of Internet constituent interests. At least two federal circuits have construed a purported ambiguity in the language of the Act so as to hold that certain kinds of ISPs are *not* required to disclose the identities of suspected infringers, when such information is sought by a copyright holder pursuant to a subpoena issued under the Act.[10] This interpretation of the Act has important ramifications because, in the absence of such a requirement, these ISPs run the risk of invasion of privacy and similar litigation by their subscribers, should the ISPs voluntarily disclose their subscribers' identities to complaining copyright holders.[11] At the same time, however, copyright holders are unlikely simply to fold their tents and forego their efforts to obtain the identities of suspected Internet infringers. Instead, in accordance with these judicial holdings, complaining copyright holders have no recourse but to pursue litigation against the ISPs; as a result, the ISPs will ultimately have no choice but to comply with their requests

---

7. *See* § 512(c)(1).

8. *See, e.g.*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., 351 F.3d 1229, 1235 (D.C. Cir. 2003) [hereinafter *Verizon III*] (explaining the compromise to be the ISP's ability to protect the rights of copyright holders while still maintaining their clientele).

9. § 512(c)(1).

10. *See Verizon III*, 351 F.3d at 1237; *see also In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 774 (8th Cir. 2005).

11. *See, e.g.*, Alice Kao, RIAA v. Verizon: *Applying the Subpoena Power of the DMCA*, 19 BERKELEY TECH. L.J. 405, 419-21 (2004) (discussing the assumption of privacy which many Internet users hold and the potential dangers of broad subpoena powers).

for subscriber identities.

The specific language in the Liability Limitation Act that caused certain courts to disrupt the delicate balance between the interests of ISPs, copyright holders, and Internet subscribers is a provision in the Act which requires a copyright holder who serves a subpoena under the statute to also provide the ISP with certain specific details regarding the nature and timing of the alleged infringing Internet distribution—the "512(c) Notice."[12] Because the kind of information called for in the 512(c) Notice appears most relevant to *locating and removing* allegedly infringing material from the Internet, these courts concluded that the incorporation of the 512(c) Notice requirement renders the Act's subpoena provisions ambiguous as to exactly what the receiving ISP is obliged to do in order to comply with the subpoena.[13] Is the ISP required to: (i) locate and remove the infringing material, *or* (ii) disclose the identity of the responsible subscriber, *or* (iii) do both? These courts resolved this purported ambiguity by deciding that the Act requires both acts of compliance. Finally, and most importantly, these courts further concluded that subpoenas issued under the Act *are therefore effective only against ISPs that can in fact perform both acts of compliance;* that is, only those ISPs that are capable of removing infringing material, as well as disclosing the identities of the subject subscribers, are required to respond to such subpoenas. On the basis of this reasoning, these courts ultimately held that ISPs that do not store (and therefore cannot remove) user transmitted material, have no obligation to comply with Liability Limitation Act subpoenas in any way. The courts reached this conclusion notwithstanding the obvious fact that these ISPs are nonetheless in possession of subscriber identification information, and are fully capable of disclosing that information in response to substantiated allegations of unauthorized file-sharing and other acts of copyright infringement.

C. An Alternative Construction of the Liability Limitation Act

While the foregoing judicial analysis of the Liability Limitation Act is a plausible one, it is also one that contravenes the express objective of the statute: that is, the expeditious disclosure of alleged infringer identities and the removal of ISPs from copyright holder/Internet user conflicts. The critical error in the reasoning of these courts is their inflexible approach in divining the legislative purpose underlying the incorporation of the 512(c) Notice into the

12. *See* § 512(c).

13. *See In re Charter*, 771 F.3d at 776-77; *Verizon III*, 351 F.3d at 1234; Interscope Records v. Does 1-7, 494 F. Supp. 2d 388, 391 (E.D. Va. 2007); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 953-56 (M.D.N.C. 2005).

Act's subpoena provisions. While the information provided pursuant to the 512(c) Notice can certainly be helpful to an ISP in locating and removing infringing material from the Internet, *this information can also be used by the ISP to assist it in identifying the subscriber who transmitted the allegedly infringing material.* Consequently there is no reason to indelibly restrict the function of the 512(c) Notice to locating and removing infringing material from the Internet (and thereby creating an impossible compliance obligation for ISPs that do not store user-transmitted material). Assessed from this perspective, the Act's subpoena provisions collectively anticipate only a single act of compliance on the part of a subpoenaed ISP: the disclosure of the identity of a subscriber who has allegedly transmitted infringing material over the Internet. In as much as it is possible to construe the language of the Liability Limitation Act in a manner consistent with its express statutory purpose, the Act should therefore be considered unambiguous, and accordingly, its subpoena provisions should be applied to all ISPs.[14]

D. A More Socially Responsible Application of the Act

Apart from the foregoing question of statutory construction of the Act, there are also social utility considerations which favor the application of its subpoena provisions to all ISPs. Some supporters of the above judicial interpretation of the Act argue that this interpretation should be upheld because the overall result provides a socially important benefit: the subordination of copyright property rights in favor of ISP subscriber free speech and privacy interests.[15] This argument, however, while facially appealing, incorrectly casts copyright protection and Internet user privacy in antagonistic social utility roles.

First, there is no right to "privately" break the law. Indeed, the fact that certain illegal conduct may be difficult to detect typically mandates that any pertinent privacy interests be specifically assessed against the possibility that lack of detection and concomitant legal redress may actually encourage the undesirable conduct. This is certainly a relevant consideration in addressing the widespread problem of illegal Internet file-sharing.

Second, legitimate privacy and free speech interests are not impaired where subscriber identities are required to be disclosed only upon a proper showing of documented infringement activity. As discussed above, when properly construed, the Liability Limitation Act's 512(c) Notice actually favors subscriber privacy. Specific details

14. *See, e.g., In re Charter*, 393 F.3d at 778, 780-83 (Murphy, J., dissenting).

15. *See, e.g., In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 257 (D.D.C. 2003) [hereinafter *Verizon II*].

regarding the nature and timing of an infringing transmission can aid an ISP in narrowing down its internal search to the culpable subscriber, thereby minimizing the possibilities of disclosure of the identities of innocent subscribers. In addition, the more information the ISP has regarding an allegedly infringing transmission, the more such information it can in turn provide to its subscriber before disclosing her identity. Armed with this information, an innocent subscriber could determine that someone with access to her computer is the real culprit or even show that neither she nor any authorized user undertook the infringing acts. In such case, she could put the complaining copyright holder on notice that if she pursues her allegations, she does so at her own peril.

Moreover, removing certain kinds of ISPs from the ambit of Liability Limitation Act subpoenas does little to enhance the legitimate privacy interests of ISP subscribers because it ultimately affords them no greater protection than that currently provided under the law. Under the Act's provisions, ISPs are not required to disclose subscriber identities in response to unsubstantiated allegations of infringement. Consequently, ISP subscribers are already afforded protection from copyright holder "infringement fishing expeditions." Additionally, copyright holders retain alternative (albeit more costly) discovery means by which to obtain subscriber identity information. Thus, restricting the use of Liability Limitation Act subpoenas only increases the costs involved in the inevitable disclosure of infringer identities. Given that in substantiated instances of infringement, the relevant subscriber identities will be eventually disclosed anyway, there is little practical or social benefit in driving up the costs of such disclosure, which will only be passed on by ISPs to their general (and mostly law-abiding) subscribers. Simply put, given that the majority of Internet users do not engage in the unauthorized file-sharing of copyrighted works, why should they have to pay for "delayed detection protection" on behalf of Internet copyright infringers?

Finally, there is little social benefit in making it easier for Internet infringers to avoid detection and legal responsibility for their actions. The ease of Internet dissemination has contributed to a growing disregard for the rights of others by some users of the Internet. In addition to infringement of intellectual property rights, Internet rights violations on the rise include defamation, fraud, infliction of emotional distress, and a legal cornucopia of tortious and other legal harms.[16] Important civil liberties such as anonymous

16. *See* Lateef Mtima, *The Changing Landscape of Internet Use and Dissemination of Copyrighted Works: New Tools, New Rules, Or The Same Old Regime?*, COMPUTER & INTERNET LAW, Oct. 2007, at 1 [hereinafter Mtima, *The Changing Landscape*] (discussing such legal harms arising from Internet infringement claims); *see also* Assaf

speech and individual privacy should not be vitiated to protect illegal acts and promote self-serving indifference to the rights of other citizens. A vibrant Internet community is just as dependent upon the preservation of traditional "brick-and-mortar" rights and mores, as it is upon novel interpretations and applications of the law.

Part I of this Article will briefly recount the early history of copyright infringement litigation between copyright holders and ISPs, and will discuss how such litigation threatened the advance of universal Internet access. It will also examine how judicial resolutions of these disputes contributed to Congress's eventual passage of the Liability Limitation Act to address this problem.

Part II will summarize the key provisions of the Liability Limitation Act, and will examine the legislative purpose in passing the statute. This Part will also explore the specific means through which the Act achieves the intended balance of ISP/copyright holder/Internet user interests with respect to the problem of Internet copyright infringement.

Part III will analyze the judicial decisions which hold that the subpoena provisions of the Liability Limitation Act do not apply to "mere conduit" ISPs, that is, ISPs which provide Internet access but do not store user-transmitted material on their servers. As discussed above, these courts arrived at their conclusions by first finding the Act's subpoena provisions to be ambiguous and contradictory, and thus in need of judicial interpretation. In deciding that the purported ambiguity places an impossible obligation upon "mere conduit" ISPs, the courts then "resolved" this ambiguity by deciding that the subpoenas provisions simply don't apply to such ISPs, and thus, these ISPs have no obligation to comply with subpoenas issued under the Liability Limitation Act.

Part IV will challenge the judicial conclusion that the subpoena provisions of the Liability Limitation Act do not apply to "mere conduit" ISPs. As a question of statutory construction, this Part will proffer that the subpoena provisions of the Act can be reasonably interpreted to extend to such ISPs. While the Act's subpoena provisions do require that a 512(c) Notice accompany the subpoena, within the context of the subpoena provisions, the function of the 512(c) Notice is not that of triggering the removal of infringing material from the Internet. Rather, in this context, the 512(c) Notice is intended to ensure the provision of information which will assist the ISP in identifying suspected infringers. Consequently there are no ambiguous or contradictory compliance obligations placed upon

---

Hamdani, *Who's Liable For Cyberwrongs?*, 87 CORNELL L. REV. 901, 943 (2002) (discussing the novel approach of finding liability for copyright infringement through direct, contributory, or vicarious tort liability).

"mere conduit" ISPs under the subpoena provisions of the Act. Because there is a plausible interpretation of the Act that renders its provisions unambiguous and preserves the statutory purpose, this alternative interpretation should be favored over a construction that contravenes the statutory goals.

Finally, Part V will argue that the notion that Congress perhaps intended to subordinate copyright property rights to Internet subscriber free speech and privacy interests in passing the Liability Limitation Act is an analytical chimera. While some commentators legitimately question whether Congress struck a *desirable* balance of free speech/privacy versus copyright property interests in passing the Act, these arguments do not alter the fact that Congress's decision to preserve the traditional curtailment of free speech/privacy interests in the preservation of copyright property rights is a proper exercise of its authority. While Congress could have afforded greater deference to Internet subscriber free speech/privacy concerns, the decision to require ISP disclosure in the face of substantiated allegations of copyright infringement does not impermissibly burden these rights. Moreover, while the Internet and related tools of digital information technology can provide great educational and cultural boons, if left irresponsibly unbridled it can also threaten some of our most cherished legal rights and social mores. Reasonable Internet regulation, including the disclosure of ISP subscriber identities when appropriate, helps to minimize the potential for abuse of this revolutionary means of human communication and expression.

Construing the Liability Limitation Act's subpoena provisions to extend to all ISPs implements the actual and legitimate legislative intent underlying the Act, and further, comports with the overarching policy goals of the copyright law as a whole. In contrast, requiring copyright holders to mire ISPs in litigation merely to obtain the identities of alleged infringers defeats the Act's purpose, and embroils ISPs in infringement disputes in which they have no immediate interest. Construing the Act's subpoena provisions to extend to all ISPs preserves an appropriate balance between the interests of ISPs, copyright holders, and Internet users, and places the responsibility for preventing or redressing Internet copyright infringement where Congress intended: on copyright holders, and on those Internet users who engage in the unauthorized distribution of copyrighted works.

I. THE EARLY INTERNET COPYRIGHT INFRINGEMENT LITIGATION FRONTIER

In the 1980s and 1990s, Americans became familiar with the brave new world of the Internet, and the heady freedom of instantaneous self-publication. For the first time, private individuals

could immediately share their personal views, opinions, and ideas with the world—and right from the comfort of their own homes.[17]

17. *See* Adrianne Goldsmith, *Sex, Cyberspace, and the Communications Decency Act: The Argument for an Uncensored Internet*, 1997 UTAH L. REV. 843, 844-45 ("The 'information superhighway' is a global system of interconnected computer networks; it offers an easy and inexpensive way for anyone with access to a computer, a modem, and a telephone line to 'instantaneously and interactively communicate' with people from around the world. The Internet is 'the largest international computer network, linking more than 40,000 independently managed computer networks, including tens of thousands of universities, laboratories, governmental entities, corporations, and individuals in over 100 countries.' The Internet is neither 'owned nor controlled by a single entity and has 'no central governing authority.' Before the federal government burst onto the scene as the self-appointed 'cybercensor,' the Internet had remained essentially self-regulated, operating by informal agreement among its subscribers and by formal agreement among local network providers." (footnotes omitted) (internal quotation marks omitted)); Lawrence Lessig, *Creative Economies*, 2006 MICH. ST. L. REV. 33, 37-38 ("[Internet use and dissemination] is digital creativity. This is digital remix. . . . Anybody with a $1,500 computer can take images and sounds from the culture around us and remix them together to express ideas and arguments more powerfully than anything any of us could write as text. This is remix with more than text, yet it is the literacy of a twenty-first century. It is what kids do with computers once they are finished hoarding all of the content that was ever produced in the history of man. When they grow bored with the hoarding, what do they do next? They find things to do with the content they've collected. And what do they do? . . . This is what they do. This is writing for them. It has extraordinary creative potential. It will change what whole fields of creativity look like. More important, it has extraordinary democratic potential—changing the freedom to speak by changing the power to speak, making it different. Not just broadcast democracy, but increasingly a bottom-up democracy. Not just the *New York Times* democracy, but blog democracy. Not just the few speaking to the many, but increasingly peer-to-peer. This is what this architecture begs for—this form of expression, then this expression set free on a free digital network that anyone in the world can access as they demand. This is the invitation that digital technologies give to our cultures."); Michael J. Madison, *Social Software, Groups, And Governance*, 2006 MICH. ST. L. REV. 153, 153 ("The 'personal computing' technology paradigm of the last twenty years has done much to expand the scope of individual agency in the context of law and policy. Computers help individuals to create and consume information at unprecedented scale and at unprecedented speed."); Lateef Mtima, Introduction, *Symposium: Intellectual Property and Social Justice,* 48 How. L.J. 571, 572 (2005) [hereinafter Mtima, Introduction] ("[T]he digital revolution and similar technological advances present unheralded opportunities though which to confront [intellectual property social inequity] from a socially redeeming vantage point. . . . [T]he new technologies can provide the apparatus through which to achieve a more equitable distribution of the benefits of creative endeavor."); Ruth Okediji, *Givers, Takers, And Other Kinds of Users: A Fair Use Doctrine For Cyberspace,* 53 FLA. L. REV. 107, 108 (2001) ("[I]nformation technology has empowered ordinary users to become part of the creative process both by its interactive nature and the very architecture of the pennon of the information society, the Internet." (footnote omitted)); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1834 (2000) ("The Internet is one of the Twentieth Century's most important innovations. The Internet's prompt, accurate, and inexpensive distribution of digital information means that practically anyone can receive or disseminate text, images, sound, software or data at the touch of a button. Indeed, a person with an

Indeed, the very ease of this revolutionary means of communication led many to believe mistakenly that if can be digitized, it can be shared:

> Starting in the 1980s, internet users began "posting" copyrighted works on electronic bulletin boards (BBSs). A BBS allows a user to post files for others to download to their computers. Other internet users would then copy and download the posted works from the BBS. Beginning in the early 1990s, copyright owners began suing individuals who unlawfully disseminated copyrighted music, photographs, and software. Such litigation targeted BBSs operated from home computers.[18]

Recognizing the real and potential threat to their economic interests, copyright holders turned to the courts for protection from this new technological means of impingement upon their intellectual property rights.[19] It soon became evident, however, that the real

---

ordinary personal computer and a modem can communicate with as many people as a major corporation with millions of dollars in resources. Now, more than ever before, practically anyone can influence the duplication and dissemination of information around the world." (footnote omitted)).

18. *In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773 (8th Cir. 2005); *see also, e.g.*, Playboy Enters. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 505 (D. Ohio 1997); Sega Enters. v. Sabella, [1996] Copyright L. Dec. (CCH) ¶ 27, 648 (N.D. Cal. Dec. 18, 1996); Sega Enters. v. Maphia, 948 F. Supp. 923, 926 (N.D. Cal. 1996); United States v. Stowe, [1996] Copyright L. Dec. (CCH) ¶ 27,625 (N.D. Ill. Aug. 14, 1996); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 923 F. Supp. 1231, 1238-39 (N.D. Cal. 1995). *See generally* Guest v. Leis, 255 F.3d 325, 329-30 (6th Cir. 2001); Yen, *supra* note 17, at 1835 ("[A]ggressive copyright enforcement strategies may not be enough to [protect copyright owners' interests]. Infringements occur because many Internet users are ignorant of copyright law. Other users deliberately infringe and hope that they will not be discovered. Even if content providers detect infringement, they often go uncompensated because the costs of pursuing compensation outweigh the expected recovery or because the infringer cannot be found." (footnotes omitted)).

19. *See, e.g.*, Kao, *supra* note 11, at 405 ("[W]hile the adoption of digital formats has opened tantalizing opportunities, these opportunities come with many costs and challenges. The same improvements in network technology, data compression, and increased availability of broadband Internet service that make possible new avenues of content distribution also facilitate duplication of content with little or no loss of quality and the wide distribution of such copies." (footnotes omitted)); Mtima, *The Changing Landscape, supra* note 16, at 4 ("Up until the digital technological revolution, the . . . division between the copyright holder's exclusive rights and the uses available to the public worked relatively well. Copyright owners routinely granted assignments and licenses of their exclusive rights to commercial users of their work, such as publishers who wished to make multiple copies and distribute them for sale to the public. Inasmuch as authors thereby authorized only the sale of individual copies of their works to the general public, they granted the public no right to engage in any of the 106 exclusive rights' activities (such as making copies) in connection with the authors' works. . . . Notwithstanding the copyright division of authors' rights and public privileges, however, the real reason that members of the public were not likely to infringe upon a copyright holder's exclusive rights, at least not in any meaningful way,

targets of much of this litigation were not the infringers themselves, but rather the entities that made access to the Internet available in the first place—Internet service providers or "ISPs."[20] Given the decentralized structure of the Internet, and the growing number of quasi-anonymous (and often judgment proof) individual infringers, this was the most viable and pragmatic strategy. In addition to their enticingly deep pockets, ISP defendants also presented the attractive prospect of a powerful ally in the war against Internet copyright infringement. If ISPs could be held responsible in connection with the copyright misconduct of their subscribers and other copyright end-users, then ISPs would have strong impetus to implement anti-infringement preventive measures and corrective policies.[21]

For their part, ISPs appealed to the courts that holding them

---

was one of basic practicality. Making multiple copies and/or engaging in the mass distribution of copyrighted material was an expensive undertaking, and one that was difficult to conceal. With the advent of digital technology, however, the practical obstacles to surreptitious copyright infringement largely disappeared. Today, possession of a single digital copy enables reproduction and distribution of a copyrighted work to an infinite number of people- and all from the privacy of a personal laptop.").

20. *See, e.g.*, Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 950-51 (C.D. Cal. 1997); Playboy Enters. v. Webbworld Inc., 991 F. Supp. 543, 552 (N.D. Tex. 1997); Religious Training Center v. Lerma, 24 Media L. Rep. (BNA) 2473, (E.D. Va. 1996); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995); Sega Enters. v. Maphia, 857 F. Supp. 679 (N.D. Cal. 1994), *modified* 948 F. Supp. 923 (N.D. Cal. 1996); Playboy Enters. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993). *See generally* Seth F. Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 87-90 (2006); David Ludwig, *Shooting the Messenger: ISP Liability for Contributory Copyright Infringement*, 2006 B.C. INTELL. PROP. & TECH. F. 110701; David Weiskopf, *The Risks of Copyright Infringement on the Internet: A Practitioner's Guide*, 33 U.S.F. L. REV. 1, 19-38 (1998); Yen, *supra* note 17, at 1840-41, 1876-80; John Borland, *ISPs Gird for Copyright Fights*, CNET NEWS, Sept. 9, 2002, http://news.cnet.com/ISPs-gird-for-copyright-fights/2100-1028_3-957023.html (discussing copyright content industry strategy of suing ISPs for subscriber infringement).

21. *See, e.g.*, Hamdani, *supra* note 16, at 911 ("The failure of subscriber-only liability to prevent cyber-misconduct is virtually undisputable, and there is a general consensus that ISPs should be harnessed to the preventive effort."); Yen, *supra* note 17, at 1836 ("Principles of enterprise liability, therefore, indicate that ISPs should internalize losses resulting from that risk as a cost of doing business. This will force ISPs to deter copyright infringement, raise compensation for copyright infringements that occur, and spread costs throughout the Internet-user community." (footnotes omitted)); Emily Zarins, *Notice Versus Knowledge Under the Digital Millennium Copyright Act's Safe Harbors*, 92 CAL. L. REV. 257, 267 (2004) ("[F]aced with liability for direct infringement regardless of knowledge, a service provider could either close up shop or feverishly try to monitor all content flowing through its infrastructure through some centralized enforcement mechanism. Naturally, a threatened service provider that survives would be more compelled to overpolice rather than to underpolice and stand vulnerable to direct infringement claims.").

liable for the infringement activities of individual Internet users would be not only unfair, but socially disastrous.[22] Holding ISPs responsible for individual Internet abuses would be akin to holding the telephone company responsible for obscene phone calls.[23] Indeed, the opportunity for uncensored individual expression and exchange is one of the inherent features of the Internet that makes it a revolutionary means of communication.[24] Thus, even if it were

---

22. *See, e.g., Sega Enters.*, 857 F. Supp. at 683. There, Sega brought suit for copyright infringement and related claims against defendants who maintained Internet electronic bulletin boards through which their subscribers bartered and traded Sega video games. *See id.* Defendants argued that they should not be held liable because they neither participated in nor were able to control their subscribers' conduct, and had no way of knowing in advance when it would occur. *See id.* at 686-87. While the court expressed some concerns with regard to hindering the development of the Internet, it nonetheless held that defendants could be held liable for *contributory* copyright infringement. *See id.*; *see also* Kreimer, *supra* note 20, at 86-87 (arguing that imposing liability upon ISPs in connection with subscriber misconduct could spur ISP censorship: "[A]lthough the DMCA erects a system that can be manipulated to induce intermediaries to censor targeted works, in form, at least, it provides protection against liability of many Internet intermediaries for unknowing contribution to copyright violations, and limits incentives for intermediaries to take initiatives to censor material passing through their facilities." (footnotes omitted)).

23. *See, e.g., Netcom*, 907 F. Supp. at 1369 n.12 ("[The ISP] Netcom compares itself to a common carrier that merely acts as a passive conduit for information. . . . Netcom would seem no more liable [for infringing end-user transmissions] than the phone company for carrying an infringing facsimile transmission or storing an infringing audio recording on its voice mail."); *see also* John Gibeaut, *Zapping Cyber Piracy*, 83 A.B.A. 60, 62 (1997); Yen, *supra* note 17, at 1836 ("The argument against [ISP] liability claims that ISPs are not responsible for their subscribers' behavior. Internet service does not necessarily imply copyright infringement; therefore, the decision to use the Internet this way and any legal responsibility properly rest with the subscriber.").

24. *See* Communications Decency Act, 47 U.S.C. § 230(a)(3) (2006) ("The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."); Reno v. ACLU, 521 U.S. 844, 870 (1997) ("[T]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."); Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1624 (1995); Goldsmith, *supra* note 17, at 868-69 ("The greatest strength of the Internet is its power to allow anyone and everyone to communicate instantaneously, without geographic limits. . . . First, the Internet presents very low barriers to entry. A person needs only a computer, a modem, and a telephone line to reach millions of people worldwide. Second, the barriers to entry are identical for everyone, unlike other methods of communication, such as the print or broadcast media, where a few players monopolize the arena. Third, the content of the material on the Internet is amazingly diverse as a result of these low barriers to entry. Finally, the Internet provides access to anyone who wishes to speak, and creates a degree of equality among the speakers. No one person has any more power or prominence on the Internet than another."

possible to screen and censor each and every individual Internet transmission, adopting such practices would eliminate the principal social utility benefit that the Internet provides.[25]

Initially, the courts struggled not only to reconcile these competing social and commercial interests, but also to apply traditional copyright principles to the novel issues raised by these disputes.[26] The results of these initial efforts, however, were often

---

(footnotes omitted)).

25. *See, e.g.*, Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) ("This ability to speak one's mind [on the Internet] without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."); Goldsmith, *supra* note 17, at 847 ("Admittedly, the government has a compelling interest in protecting the safety, welfare, and morals of both children and adults. But any content-based restriction of speech or expression must be narrowly tailored to further that compelling interest. If the regulation sweeps too broadly, it may encompass protected as well as unprotected speech, thus violating the freedom of speech guaranteed by the First Amendment. The Framers of the Constitution 'fashioned the First Amendment's protection of free speech and press to ensure the continual exchange of political ideas and social sentiment.' An uncensored Internet epitomizes the free forum envisioned by the Framers of the Constitution." (footnotes omitted)); Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 860-61 (2000) ("The promise of the Internet is empowerment: it empowers ordinary individuals with limited financial resources to "publish" their views on matters of public concern. The Internet is therefore a powerful tool for equalizing imbalances of power by giving voice to the disenfranchised and by allowing more democratic participation in public discourse. In other words, the Internet allows ordinary John Does to participate as never before in public discourse, and hence, to shape public policy. Yet, [Internet defamation] suits . . . threaten to reestablish existing hierarchies of power, as powerful corporate Goliaths sue their critics for speaking their minds. . . . Thus, these Internet defamation actions threaten not only to deter the individual who is sued from speaking out, but also to encourage undue self-censorship among the other John Does who frequent Internet discussion fora." (footnotes omitted)).

26. *See, e.g.*, Religious Tech. Ctr. v. Lerma, 24 Media L. Rep. (BNA) 2473, 2476 (E.D. Va. 1996) ("While the Internet does present a truly revolutionary advance, neither Congress nor the courts have afforded it unique status under the [copyright laws]. The law of copyright has evolved with technological change, with each new technological advancement creating complicated questions of copyright interpretation and application. Nevertheless, the new technologies—from television, to videocassette recorders, to digitized transmissions—have been made to fit within the overall scheme of copyright law and to serve the ends which copyright was intended to promote. . . . The Internet is no exception, and postings on it must be judged in reference to the already flexible considerations which fair use affords." (citation omitted)). *See generally* Lateef Mtima, Tasini *and Its Progeny: The New Exclusive Right or Fair Use on the Electronic Publishing Frontier?*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 369, 371-72 (2004) [hereinafter Mtima, Tasini *and Its Progeny*] ("Distilling concrete and comprehensive directives from copyright/new technology litigation disputes has never been easy. . . . Interpreting and adapting copyright canons and license terms developed in connection with traditional uses for copyrighted material, to account for revolutionary technological advances, is an inevitably incremental and iterative process." (footnote omitted)).

confusing and inconsistent, providing little guidance to copyright holders or ISPs in structuring and protecting their legal and business interests.[27]

Eventually, in the seminal case of *Religious Technology Center v. Netcom On-Line Communication Services,* the District Court for the Northern District of California laid the foundation for a pragmatic application of traditional copyright principles to the thorny problem of Internet infringement liability.[28] In *Netcom*, the Church of Scientology brought suit against a former Scientology Minister, who had made unauthorized postings of copyrighted Scientology texts to an electronic bulletin board.[29] The Church also named the operator of the bulletin board and the ISP, Netcom, as defendants in the suit.[30]

---

27. *See* Lateef Mtima, *Copyright Controversies in the Digital Age, in* A.L.I./A.B.A. Coursebook: INTERNET LAW FOR THE PRACTICAL LAWYER 83, 90 (2007) [hereinafter Mtima, *Copyright Controversies*] ("The absence of detailed substantive analyses of direct infringement in the Internet copyright context in many of the early Internet copyright cases has resulted in an unusually vague and unsettled legal landscape in this area."); Michelle A. Ravn, *Navigating Terra Incognita: Why the Digital Millennium Copyright Act Was Needed to Chart the Course of Online Service Provider for Copyright Infringement*, 60 OHIO ST. L.J. 755, 759 (1999) ("Prior to the enactment of the DMCA, the few federal court opinions which addressed OSP liability attempted to apply traditional copyright principles of vicarious and contributory liability. Offering little guidance to future courts eagerly in search of precedent as they sought to apply the existing copyright law to an environment characterized by changing technology, these courts reached divergent and sometimes confusing conclusions."). Consider also, for example, *Playboy Enters. v. Frena*, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993), wherein Playboy brought an action for copyright and trademark infringement against a bulletin board operator who permitted subscribers to upload and download Playboy pictures from his site. *Id.* Although the defendant argued that he had been unaware of his subscribers' activities and, that once he became aware he took steps to prevent further infringement, the court nonetheless held the defendant liable for *direct* infringement: "There is irrefutable evidence of direct copyright infringement in this case. It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature." *Id.* at 1559. *See generally* Lateef Mtima, *Trademarks, Copyrights, and the Internet, in* TRADEMARKS, COPYRIGHT, AND UNFAIR COMPETITION FOR THE GENERAL PRACTITIONER AND THE CORPORATE COUNSEL 365 (ALI-ABA 2004) (reviewing cases where liability was found for unauthorized Internet publication of copyrighted material, including *Frena*).

28. 907 F. Supp. 1361 (N.D. Cal. 1995).

29. *Id.* at 1365-66.

30. *Id.* at 1361. The facts of the case belie the contentious state of affairs regarding Internet infringement disputes in the pre-DMCA era:

> After failing to convince [former minister] Erlich to stop his postings, plaintiffs contacted [the bulletin board operator] Klemesrud and Netcom. Klemesrud responded to plaintiffs' demands that Erlich be kept off his system by asking plaintiffs to prove that they owned the copyrights to the

In resolving the dispute, the court first undertook to harmonize prior case law regarding exactly who should be held liable (and for what) in connection with Internet copyright infringement.[31] The court began by reviewing the distinctions between the traditional theories of copyright infringement liability (i.e., direct, contributory, and vicarious infringement) all of which are implicated in unauthorized Internet transmissions.[32] With regard to liability for *direct* infringement, the court dismissed the claims against Netcom and the BBS operator, because unlike the defendant former minister, neither of these defendants had personally transmitted plaintiff's materials, or infringed upon any of the Church's other § 106 exclusive rights:[33]

> The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement.[34]

---

works posted by Erlich. However, plaintiffs refused Klemesrud's request as unreasonable. Netcom similarly refused plaintiffs' request that Erlich not be allowed to gain access to the Internet through its system. Netcom contended that it would be impossible to prescreen Erlich's postings and that to kick Erlich off the Internet meant kicking off the hundreds of users of Klemesrud's BBS. Consequently, plaintiffs named Klemesrud and Netcom in their suit against Erlich, although only on the copyright infringement claims.

Id. at 1366 (footnote omitted). Virtually all of these preliminary matters are now governed by express provisions in the Online Copyright Liability Act. *See infra* Part II.

31. *Netcom*, 907 F. Supp. at 1368-72.

32. *Id.*; *see* 3 NIMMER ON COPYRIGHT § 12.04 (2008).

33. *Netcom*, 907 F. Supp. at 1366-67 ("Infringement occurs when a defendant violates one of the exclusive rights of the copyright holder." (citation omitted)); *see* 17 U.S.C. § 106 (2006); Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 546-47 (1985) ("Section 106 of the Copyright Act confers a bundle of exclusive rights to the owner of the copyright. Under the Copyright Act, these rights—to publish, copy, and distribute the author's work—vest in the author of an original work from the time of its creation." (footnote and citation omitted)); Perfect 10, Inc., v. CCBill, LLC, 481 F.3d 751, 768 (9th Cir. 2007).

34. *Netcom*, 907 F. Supp. at 1369; *see also* Parker v. Google, Inc, 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006) ("When an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition [for direct infringement] is missing. . . . It is clear that . . . automatic archiving . . . and [caching] of websites in [response] to users' search queries do not include the necessary volitional element to constitute direct copyright infringement." (footnote omitted)); Playboy Enters. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 512-13 (N.D. Ohio 1997) (holding that because setting up an electronic bulletin board is not an exclusive right under 17 U.S.C. § 106 a party who does no more than that cannot be liable for direct infringement, although the court found infringement by defendants on other grounds).

On the other hand, the court held that with respect to the Church's claims based on *contributory* infringement, which requires a finding of knowledge of the infringing activity,[35] and the claims based on *vicarious* liability, which requires a finding that the defendant had the right and ability to control the infringing activity and received a direct financial benefit from that activity,[36] the Church had at least raised an issue of fact as to whether Netcom and the bulletin board operator had aided and abetted the former minister's infringement conduct.[37]

> [T]he evidence reveals a question of fact as to whether Netcom knew or should have known that [former minister] Erlich had infringed plaintiffs' copyrights following receipt of plaintiffs' letter [complaining of infringement]. Because Netcom was arguably participating in Erlich's public distribution of plaintiffs' works, there is a genuine issue as to whether Netcom knew of any infringement by Erlich before it was too late to do anything about it. If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement since its failure to simply cancel Erlich's infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in Erlich's public distribution of the message.[38]

---

35. *See* 3 NIMMER ON COPYRIGHT § 12.04 (2008); *see also, e.g.*, Warner Bros. Records, Inc. v. Souther, No. 1:05CV279, 2006 WL 1549689, at *2 (N.D.N.C. June 1, 2006) ("A person may also be held to account for actions of others who violate copyright laws. Under the doctrine of contributory copyright infringement, a person may be held liable for 'contributory infringement' if with knowledge of the infringing activity, that person 'induces, causes or materially contributes to the infringing conduct of another . . . . Put differently, liability exists if the defendant engages in personal conduct that encourages or assists the infringement.' Thus, the essential elements of contributory copyright infringement are, as follows: (1) knowledge, and (2) material contribution." (alteration in original) (citations omitted)); Adobe Syst., Inc. v. Canus Prods., Inc., 173 F. Supp. 2d 1044, 1048 (C.D. Cal. 2001).

36. *See* 3 NIMMER ON COPYRIGHT § 12.04[A][2] (2008); *see also, e.g.*, *Netcom*, 907 F. Supp. at 1376 ("[To recover on a theory of vicarious infringement, p]laintiffs must further prove that Netcom receives a direct financial benefit from the infringing activities of its users. For example, a landlord who has the right and ability to supervise the tenant's activities is vicariously liable for the infringements of the tenant where the rental amount is proportional to the proceeds of the tenant's sales. However, where a defendant rents space or services on a fixed rental fee that does not depend on the nature of the activity of the lessee, courts usually find no vicarious liability because there is no direct financial benefit from the infringement." (citation omitted)).

37. *Netcom*, 907 F. Supp. at 1374.

38. *Id.* The court made similar findings in connection with the defendant bulletin board operator. *Id.* at 1381-82; *see also* Faulkner v. Nat'l Geographic Soc'y, 211 F. Supp. 2d 450, 472-74 (S.D.N.Y. 2002); *Russ Hardenburgh*, 982 F. Supp. at 514 (finding contributory infringement where defendants "clearly induced, caused, and materially contributed to any infringing activity which took place on their [bulletin board]."); Playboy Enters., v. WebWorld, Inc., 968 F. Supp. 1171, 1174-75 (N.D. Tex. 1997), *modified*, 991 F. Supp. 543 (N.D. Tex. 1997) (finding that where defendant ISP had

Albeit an insightful application of the copyright law to the Internet context, the *Netcom* opinion provided only limited comfort to commercial Internet litigants. While copyright holders could relish in the fact that ISPs were not immunized from indirect liability all together, the prospect of having to demonstrate actual knowledge and/or direct financial benefit on the part of ISPs was not an attractive one. As for ISPs, while the *Netcom* analysis limited their exposure, it did not entirely extricate them from onerous and costly copyright infringement litigation and discovery. Like the judgments of King Solomon, the *Netcom* decision rendered no jubilant victor.[39]

Nonetheless, the *Netcom* decision did point the way toward a pragmatic compromise that would protect the rights of copyright holders without hindering the development of the Internet. If ISPs could only be held liable for knowing or active participation in the infringement conduct of their subscribers, legislators could establish legal parameters for determining when ISP services could be deemed to have met this threshold. Thus the *Netcom* analysis ultimately provided the analytical basis for the Online Copyright Liability Limitation Act, which largely extinguishes ISP vicarious or indirect

---

collected, packaged and even modified Playboy images submitted by its subscribers, ISP was liable for direct infringement). In *WebWorld*, the court reasoned that defendant "did not sell access [to the Internet]; it sold adult images. . . . [Defendant] did not function as a passive conduct of unaltered information. Instead, [defendant] functioned primarily as a store, a commercial destination within the Internet. Just as a merchant might repackage and sell merchandize from a wholesaler, so did [defendant] re-package (by deleting text and creating [thumbnail versions]) and sell images it obtained from the various news groups. In contrast to [mere Internet access providers defendant] took 'affirmative steps to cause the copies to be made.'" 991 F. Supp. at 552 (citation omitted). The court in *WebWorld* also levied judgments against the corporate defendant's individual operators for vicarious copyright infringement. *See id.* at 554; *see also* Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004) (explaining contributory infringement); *Souther*, 2006 WL 1549689, at *2 (stating that a defendant's denial of participation in direct infringement creates an issue of fact, to be clarified through discovery and potentially resolved through summary judgment.); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1168-74 (C.D. Cal. 2002). *But cf.* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, No. C 04-0371 JW, 2004 WL 1773349 (N.D. Cal. 2004) (providing "neutral" financial services to owners of infringing website is not a basis for contributory or vicarious liability).

39. *See, e.g.*, Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 45-46 (2003); Craig A. Grossman, *From* Sony *to* Grokster, *The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War Between Content and Destructive Technologies*, 53 BUFF. L. REV. 141, 180-90 (2005); Cassandra Imfeld and Victoria Smith Ekstrand, *The Music Industry and the Legislative Development of the Digital Millennium Copyrights Act's Online Service Provider Provision*, 10 COMM. L. & POL'Y 291, 302-03 (2005); Alex Pisarevsky, *COPE-ing With The Future: An Examination of the Potential Copyright Liability of Non-Neutral Networks for Infringing Internet Content*, 24 CARDOZO ARTS & ENT. L.J. 1359, 1380-81 (2007).

infringement liability for ISP subscriber misconduct.[40] As detailed in Part II, both ISPs and copyright holders alike would now have at least concrete, if not always pristine guidelines by which to determine when an ISP might be held responsible for the infringement conduct of individual Internet users.

II. THE PASSAGE OF THE ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION ACT

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA) and thereby amended various aspects of the copyright law, in an effort to address some of the novel copyright challenges presented by advances in digital information technology.[41] The Online Copyright Infringement Liability Limitation Act, Title II of

---

40. *See Netcom*, 907 F. Supp. at 1372-73 ("Where the infringing subscriber is clearly directly liable for the [infringing] act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. Such a result is unnecessary as there is already a party directly liable for causing the copies to be made. . . . The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from non-infringing bits."). Of course, legal scholars also contributed to the shaping of intellectual property legal norms for the Internet. *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 997, 1007 (1994) ("Suppose a cyberspace user receives an interesting personal message by electronic mail from a friend. This recipient decides to forward a copy of the message, also by electronic mail, to a third party. The third party, who does not know the message's author, then decides to forward the message to all the members of an on-line discussion group. . . . Does the original author of the message, who, let us say, is unhappy and surprised by this extensive publication of the message, have a cause of action against either the friend or the third party? . . . Copying and forwarding mail is a common practice in cyberspace, but many cyber residents have not considered its possible unlawfulness and would doubtless be puzzled if they did. To be sure, there are laws of privacy and copyright in 'real'" space, but they were designed for a world in which copying a message to thousands of people took considerable time, effort and expense, and naturally gave the would-be forwarder pause for thought about issues such as privacy and copyright. . . . Now comes [an additional] new wrinkle: does the cause of action also extend to the system administrator as defendant? Should the administrator, at some time in that . . . period when he had ample opportunity to do so, have read and deleted the message or at least returned it to the sender with an explanatory note? . . . It is not feasible for the system administrator of . . . a large system actually to look at every file uploaded, nor is there a reliable method of computer screening for these files. For that matter, there is no reliable method of manual screening, even if the system administrator could take the time to do so. A user could easily upload a third party's copyrighted short story, for example, claiming it as his own. How would the system administrator know whether it was the uploader's original work or not?" (footnotes omitted)).

41. *See* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1098 (W.D. Wash. 2004).

the DMCA[42] was adopted to address the specific problem of attributing liability for Internet copyright infringement:

> Congress enacted the DMCA in an effort to resolve the unique copyright enforcement problems caused by the widespread use of the Internet. Tackling copyright infringement on the Internet required balancing the competing interests of several groups. The first set of competing interests includes those of copyright holders and end users. The DMCA "intended to 'balance the need for rapid response to potential infringement with the end-users [sic] legitimate interests in not having material removed without recourse.'" The second set of competing interests were those of copyright holders and ISPs whose services may be used to infringe copyrights. The DMCA intended to balance the interests of these parties by creating a mechanism for rights holders to inform ISPs of potentially infringing conduct while, at the same time, providing "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[43]

The principal objective of the Liability Limitation Act is to achieve a socially propitious balance between the rights and interests of copyright holders, Internet copyright end-users, and ISPs. The DMCA is designed to advance two important priorities: "to maintain strong protection for intellectual property and promote the development of electronic commerce and the technologies to support

---

42. Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified at 17 U.S.C. § 512 (1998)).

43. *Corbis*, 351 F. Supp. 2d at 1098 (quoting Rossi v. Motion Picture Ass'n of America, 391 F.3d 1000, 1003 (9th Cir. 2004) (citations omitted)); *see also* Ravn, *supra* note 27, at 759 ("The release of The White Paper, the first articulation by any presidential administration regarding the relationship between intellectual property law and the Internet, spurred additional, divergent approaches to the problem of OSP copyright infringement liability. While OSPs supported legislative efforts to minimize their liability, critics of such legislation believed it would eliminate any incentive for OSPs to discourage copyright infringement on their systems. Most commentators agreed that a delicate balance must be struck which provided protection of copyrights in cyberspace without stunting the Internet's growth . . . ." (footnotes omitted)); Katherine Raynolds, Comment, *One Verizon, Two Verizon, Three Verizon, More?—A Comment:* RIAA v. Verizon *and How the DMCA Subpoena Power Became Powerless*, 23 CARDOZO ARTS & ENT. L.J. 343, 347-48 (2005) ("Congress constructed the Digital Millennium Copyright Act . . . with a dual purpose in mind—it sought the need to limit the liability of service providers while providing copyright owners broad protection of copyrights on the Internet. The statute offers liability protection to service providers and remedies against infringement to copyright owners. Upon its creation, the DMCA was intended to be a solution that allows cooperation between copyright owners and those who have the capacity to prevent ongoing infringement." (footnotes omitted)). *See generally* Tyler T. Ochoa, *1984 And Beyond: Two Decades of Copyright Law*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 167, 179 (2003) (discussing contributory infringement and vicarious liability of ISPs); Borland, *supra* note 20 (discussing the practice of holding ISPs responsible for infringement committed by their subscribers).

that commerce."[44] Furthermore,

> Title II of the DMCA was the product of lengthy negotiations between copyright owners and internet service providers. It was designed to strike a balance between the interests of ISPs in avoiding liability for infringing use of their services and the interests of copyright owners in protecting their intellectual property and minimizing online piracy."[45]

A. *The Safe Harbor Provisions of the Online Copyright Liability Limitation Act*

The Liability Limitation Act achieves the intended Internet copyright constituent equipoise by establishing certain "safe harbor" parameters for the provision of ISP services. ISPs that abide by these guidelines can routinely provide Internet services, secure in the knowledge that they will not be held responsible for the copyright infringement activities of their subscribers or other end-users of copyrighted material.[46] At the same time, copyright holders remain

---

44. H.R. REP. NO. 105-551, pt. 2, at 18 (1998).

45. *In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 774 (8th Cir. 2005). *See generally* JAY DRATLER, JR., CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 6.05 (2008) (discussing the use of subpoenas to determine the identities of alleged infringers); Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-To-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 28 (2005) ("The DMCA safe harbor regime, adopted by Congress in 1998, reflects a compromise between the demands of copyright owners, on the one hand, and the concerns of the Internet industry, on the other hand. The Internet industry sought immunity but managed only to achieve a regime that enhances 'certainty . . . with respect to copyright infringement liability online.' For copyright owners the DMCA offered a more effective mechanism for enforcing their rights." (quoting S. REP. NO. 105-190, at 2 (1998) (footnotes omitted))); David Gorski, *The Future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in Light of the* Verizon Cases, 24 REV. LITIG. 149, 156 (2005) ("Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements . . . . At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities." (quoting S. REP. NO. 105-190, at 20 (1998))); Doris Estelle Long, *Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 533, 535-36 (2005) ("It is easy to forget that the DMCA was originally crafted as a compromise between copyright owners and internet service providers to assure both continuing protection of copyright owners' property rights, and continuing growth of the internet." (footnote omitted)).

46. *See* S. REP. NO. 105-190, at 40 (1998) ("The liability of on-line service providers and Internet access providers for copyright infringements that take place in the on-line environment has been a controversial issue. Title II of the Digital Millennium Copyright Act addresses this complex issue. Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for

free to pursue individual infringers, as well as ISPs who fail to conduct their activities within the safe harbor parameters of the Act.[47]

The Liability Limitation Act's provisions fall into two categories of application. First, there are the actual safe harbor provisions, which are "function specific."[48] That is to say that these provisions are constructed around the principal methods of providing or performing Internet services or functions.[49] "Each safe harbor applies to a particular ISP function."[50] Accordingly, each safe harbor is

---

infringements that may occur in the course of their activities."); 3 NIMMER ON COPYRIGHT § 12B.09[A] (2008); *see also Corbis*, 351 F. Supp. 2d at 1098 ("The DMCA gives an Internet service provider . . . extensive protection against liability, and leaves copyright owners with only limited injunctive relief."); Kao, *supra* note 11, at 409-10 ("The creation of these safe harbors was considered necessary because, pre-DMCA, the application of traditional copyright principles often led courts to impose liability on ISPs for the acts of their users, even those over which they had no control, threatening to stall the expansion of the Internet." (footnote omitted)).

47. *See* H.R. REP. NO. 105-551, pt. 2 at 41; S. REP. NO. 105-190, at 19; *see also Corbis*, 351 F. Supp. 2d at 1098-99 ("In addition to these notice and take down provisions, the DMCA also establishes several "'safe harbors'" that protect certain common activities of ISPs. The DMCA safe harbors do not render a service provider immune from copyright infringement. They do, however, protect eligible service providers from all monetary and most equitable relief that may arise from copyright liability. Thus, even if a plaintiff can show that a safe harbor-eligible service provider has violated her copyright, the plaintiff will only be entitled to the limited injunctive relief set forth in 17 U.S.C. § 512(j)." (citations omitted)); *Verizon III*, 351 F.3d at 1234; Jane C. Ginsburg, *Separating the* SONY *Sheep From the* Grokster *Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 580, 592 (2008); Ravn, *supra* note 27, at 787-89; Lisa Veasman, *"Piggy Backing" on the Web 2.0 Internet: Copyright Liability and Web 2.0 Mashups*, 30 HASTINGS COMM. & ENT. L.J. 311, 323-24 (2008) ("Because of the frustration between the online community and copyright owners, Congress enacted the DMCA as a compromise between these competing forces. Under section 512(c) of the Copyright Act, OSPs can avoid liability for infringing material residing on their systems at the behest of users. To qualify for protection under section 512(c), the OSP must meet several requirements: (1) the OSP cannot have "'actual knowledge'" that the infringing material is on its system; (2) the OSP must be unaware "'of facts or circumstances from which infringing activity is apparent';" (3) the OSP must promptly "'remove, or disable access to, the material'" upon notification or obtaining knowledge of the infringing activity; (4) the OSP must not receive any financial benefit from the infringing activity if it controls such activity; and (5) the OSP must have designated an agent to receive notifications of copyright infringement on its system. Additionally, the OSP must accommodate and avoid interference with "'standard technical measures,'" which copyright owners use to detect and guard against copyrighted infringement of their works." (footnotes omitted)).

48. *See* § 512(n).

49. *See In re Charter*, 393 F.3d at 775.

50. *Id.*; *see* § 512(n) ("Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service

available only to ISPs that engage in the functions or activities described in the subject safe harbor provision.[51]

In addition to the specific safe harbor provisions, the Act also contains various general conduct and liability limitation provisions that apply to all ISPs, regardless of the specific kind of Internet service or function they provide.[52] An ISP seeking immunity from liability for end-user infringement must comply with both the appropriate "function specific" provision (as determined by the nature of the ISP's service or function activities) and also any relevant general conduct provisions.[53]

B. The "Function Specific" Safe Harbor Provisions

The "function specific" safe harbor provisions of the Act, enumerated in sub-sections 512(a) through (d), are designed to ensure that ISPs conduct their activities responsibly, in light of the *particular* services they provide:

> The "safe harbor" provisions of Sections 512(a)-(d) give limited protection from copyright liability to four types of "service providers." Subsection (a) addresses transitory digital network communications or service providers who simply allow information to pass through their systems from one user of the service to another person; (b) covers system caching or providers that temporarily store data from one user before passing it on to another person at the request of the user; (c) deals with providers that allow users to store data on the provider's system or network for longer periods of time; and (d) speaks to providers that maintain data on their network or system for use with an information location tool or service. Upon compliance with various requirements set out in their respective portions of the statute, all four types of providers may gain immunity from liability for copyright infringing information that passes through or is stored on their networks or systems by [end-]users.[54]

In short, the Act's "function specific" safe harbor provisions essentially divide ISPs into two general classes.[55] The first class is composed of ISPs that are often referred to as "mere conduits," because these ISPs only provide basic access to the Internet, and allow end-user material to pass through their systems from one end-

---

provider qualifies for the limitations on liability under any other such subsection.").

51. *See* § 512(n).

52. *Id.*

53. *See Corbis*, 351 F. Supp. 2d at 1099 ("Once the threshold [general conduct] conditions have been met, a service provider must then satisfy the specific requirements for the particular safe harbor.").

54. *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 948-49 (M.D.N.C. 2005) (citation omitted).

55. *See* § 512(a)-(d).

user to another without storing such material on the ISP's servers.[56] The "function specific" safe harbor provisions that apply to such "Conduit ISPs" are set forth in sub-section 512(a) of the Act.[57]

The second class of ISPs under the Act consists of those ISPs who in some way store or otherwise maintain end-user transmitted material on their systems.[58] Under the Act, such "Storage ISPs" are further sub-categorized by the *type* of storage activity they undertake: temporary storage, storage for longer periods, or storage or maintenance activity in connection with the use of information location tools.[59] The "function specific" safe harbor provisions which apply to Storage ISPs are respectively set forth in sub-sections 512(b), (c), and (d).[60]

The Act's "function specific" safe harbor provisions distinguish between Conduit ISPs and Storage ISPs, because each of these types of ISPs can potentially affect the rights of copyright holders in different ways.[61] In this context, Conduit ISPs might best be compared with the telephone company, in that they exercise no control over the information that end-users transmit. A Conduit ISP has no foreknowledge of an end-user's infringement intentions or activities, and even after infringing material has been transmitted (including posts to non-transient websites or blogs) a Conduit ISP is unable to recall or remove such material. Until a Conduit ISP has been informed of an end-user's infringement misconduct, there is little it can do to protect the rights of copyright holders, and even then, the most it can do is disconnect the infringer. Consequently, the safe harbor provisions of sub-section 512(a) reflect these realities, and require only that Conduit ISPs disable the Internet connections of subscribers who use the ISP's service to engage in infringing misconduct.[62]

In contrast, ISPs which qualify as Storage ISPs under sub-sections 512(b), (c), or (d) have a broader range of responsive options available to them for dealing with end-user copyright infringement.

---

56. *See* § 512(a); Perfect 10, Inc. v. CCBill, LLC, 481 F.3d 751, 764-65 (9th Cir. 2007) (discussing intermediary Internet conduits: "[I]ntervening computers provide transient connections among users. The Internet as we know it simply cannot exist if those intervening computers must block indirectly infringing content."); Parker v. Google, Inc., 422 F. Supp. 2d 492, 498 (E.D. Pa. 2006).

57. *See* § 512(a).

58. *See* § 512(b)-(d).

59. *See id.*

60. *See id.*; *In re* Charter Commc'ns, Inc., 393 F.3d 771, 775 (8th Cir. 2005); *Parker*, 422 F. Supp. 2d at 498 (discussing ISP automatic storage functions, such as caching); *see also Perfect 10*, 481 F.3d at 765-66.

61. *See* § 512(a).

62. *See* § 512(i)(1)(A).

A Storage ISP may be able to disconnect a subscriber, remove infringing material from the Internet, or both.[63] Consequently, the safe harbor provisions of sub-sections 512(b), (c), and (d) all incorporate the above referenced 512(c) Notice provision, which is intended to facilitate the removal by Storage ISPs of infringing material from the Internet. As detailed below, in addition to disclosing the identities of alleged Internet infringers, Storage ISP's are further required to "respond expeditiously" to information supplied pursuant to a § 512(c) Notice, by acting to remove or disable Internet access to any such infringing material.[64]

In sum, under the "function specific" safe harbor provisions, both Conduit ISPs and Storage ISPs are eligible for immunity from liability for Internet end-user copyright infringement; however, the conditions of immunity differ, and are fashioned around the nature of the service or function provided or performed by the ISP. In this way, the Act ensures that ISPs act responsibly to address end-user infringement, while at the same time, it relieves ISPs of impossible obligations (such as preventing the transmission of infringing material in the first place, or in the case of Conduit ISPs, removing infringing material from the Internet) or other duties that would unduly hamper their ability to provide Internet service to the public.

C. The General Conduct Provisions

In addition to the "function specific" safe harbor provisions contained in sub-sections 512(a) through (d), the Act also contains general conduct and liability limitation provisions in sub-sections

---

63. *See, e.g.*, Interscope Records v. DOES 1-7, 494 F. Supp. 2d 388, 391 (E.D. Va. 2007) ("Upon receipt of the notice, Subsection (b)-(d) ISPs must respond 'expeditiously to remove, or disable access to, the material that is claimed to be infringing,' to satisfy their safe harbor requirements." (citation omitted)). In some cases, an ISP provides more than one kind of ISP service, and accordingly, is eligible for immunity under multiple safe harbors. *See* § 512(n).

64. *See* § 512(b)-(d); *Verizon III*, 351 F.3d at 1234 (Once properly notified, a service provider must "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing." (citation omitted)); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 948 (M.D.N.C. 2005) ("If a service provider fails to take down the potentially infringing material, it exposes itself to copyright liability."). The obligation to remove infringing material is set forth in subsection 512(c) and cross-referenced in subsections 512(b) and (d). *See id.* at 948-49 ("These three subsections all contain a requirement that [ISPs] respond to a written notification described in *subsection (c)(3).*" (emphasis added) (footnote omitted)); *see also Verizon III*, 351 F.3d at 1237 ("[B]ecause §§ 512(b) and (d) also require a copyright owner to provide a '"notification . . . as described in [§ 512](c)(3),"' the cross-references to § 512(c)(3)(A) in § 512(h) can not confine the operation of § 512(h) solely to the functions described in § 512(c), but must also include, at a minimum, the functions described in §§ 512(b) and (d).").

512(e) through (n), which apply to all ISPs.[65] For example, sub-section 512(i) requires all ISPs to adopt and implement express "anti-infringement" policies, and to inform their subscribers accordingly.[66] Compliance with this requirement provides an ISP with a "presumption of non-participation" in specific acts of end-user infringement, at least until such conduct is actually brought to the ISP's attention.[67]

One of the most important general conduct provisions is contained in sub-section 512(h), which authorizes copyright holders to obtain the identities of alleged infringers by serving an ISP with a subpoena (Section 512 Subpoena).[68] Among other things, sub-section

---

65. *See, e.g.*, Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1099 (W.D. Wash. 2004) ("A service provider that does not meet these threshold conditions may not invoke the DMCA's safe harbor limitations on liability.").

66. *See* § 512(i); *Corbis*, 351 F. Supp. 2d at 1100 ("A service provider must: 1) adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances; 2) inform users of the service policy; and 3) implement the policy in a reasonable manner.").

67. *See* ALS Scan, Inc. v. Remarq Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001); *In re Subpoena*, 367 F. Supp. 2d at 948; *see also Perfect 10*, 481 F.3d 751, 758 (9th Cir. 2007) ("[A] service provider 'implements' [an anti-infringement] policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications."). *But cf.* Ellison v. Robertson, 357 F. 3d 1072, 1075-80 (9th Cir. 2004) (finding that the failure to provide updated infringement notification email address creates an issue of fact as to whether ISP has implemented an anti-infringement policy); *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002) (finding that anti-infringement policy is not effectively implemented if service provider actively blocks collection of information).

68. Section 512(h) provides as follows:

> (h) Subpoena to identify infringer.
>
> (1) Request.—A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.
>
> (2) Contents of request.—The request may be made by filing with the clerk—
>
> (A) a copy of a notification described in subsection (c)(3)(A);
>
> (B) a proposed subpoena; and
>
> (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.
>
> (3) Contents of subpoena.—The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

512(h)(2)(A) directs that when serving a subpoena, the copyright holder must also provide the ISP with a 512(c) Notice, as well as an affidavit attesting that the copyright holder is seeking the ISP subscriber's identity in order to protect her copyrights.[69] These additional requirements help to ensure that Section 512 Subpoena's are used to protect legitimate copyright interests, and not to abuse the rights of copyright end-users.

For some time now, the Liability Limitation Act's safe harbor schema has provided a workable balance between the rights and interests of copyright holders, Internet copyright end-users, and ISPs.[70] Rather than routinely commence litigation against ISPs,

---

(4) Basis for granting subpoena.—If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena.—Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena.—Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

§ 512(h).

69. *Id.* As discussed below, the requirement that a section 512(c) Notice accompany a Section 512 Subpoena is what caused certain courts to question whether the subpoena provision was intended by Congress to be a "function specific" provision, applicable only to Storage ISPs, or a general conduct provision, and thus one applicable to all ISPs.

70. *See, e.g., Verizon III*, 351 F.3d at 1232 ("The RIAA has used the subpoena provisions of § 512(h) of the Digital Millennium Copyright Act (DMCA) to compel ISPs to disclose the names of subscribers whom the RIAA has reason to believe are infringing its members' copyrights. Some ISPs have complied with the RIAA's § 512(h) subpoenas and identified the names of the subscribers sought by the RIAA. The RIAA has sent letters to and filed lawsuits against several hundred such individuals, each of whom allegedly made available for download by other users hundreds or in some cases even thousands of .mp3 files of copyrighted recordings." (citation omitted)); Arista Records, Inc. v. MP3Board, Inc., No. 00 Civ. 4660, 2002 U.S. Dist. LEXIS 16165, at *1-42 (S.D.N.Y. 2002); Kreimer, *supra* note 20, at 23-24 ("In the area of intellectual property, an array of initiatives has targeted intermediaries in the effort to suppress particular varieties of content distributed over the Internet. Congress has provided strong incentives under the DMCA for ISPs, search engines, and other intermediaries to take down or block access to websites that are alleged to contain content that infringes intellectual property rights; these incentives have been deployed to induce

copyright holders have instead exercised their rights under the Act to obtain the removal of infringing material from the Internet and/or the identities of alleged infringers, effectively extricating ISPs from any ensuing infringement litigation.[71] As discussed herein, however, the balance of rights and interests achieved by the Act may be imperiled, as some courts have determined that one of the Act's salient general conduct provisions, the Section 512 Subpoena provision, does not apply to an important category of ISPs: Conduit ISPs.[72] These decisions, and the analyses upon which they are based, are discussed in Part III.

III. JUDICIAL MISCONSTRUCTION OF THE SECTION 512 SUBPOENA PROVISION

For the past several years, copyright holders have utilized the Section 512 Subpoena mechanism to obtain from various ISPs, including Conduit ISPs, the identities of alleged infringing ISP subscribers.[73] The ability to obtain expeditiously the "brick and mortar" identities of suspected Internet copyright infringers has proved an important tool in the efforts of copyright holders to undertake direct litigation against individual infringers, thereby minimizing ISP involvement in such disputes.[74]

Recently, however, some courts have questioned the breadth of the Section 512 Subpoena's reach. Beginning in 2002, the Recording Industry Association of America (RIAA)[75] sought to obtain the identities of certain suspected infringers from ISP Verizon Internet

---

intermediaries to block access to other, noninfringing content objectionable to copyright holders. Content owners have sought to push their legal entitlements further, asserting a right to unilaterally require ISPs to reveal the identity of subscribers who are alleged to violate intellectual property rights. They have sought the imposition of secondary liability to effectively oblige software and network providers to monitor their networks for infringing content, as well as regulatory initiatives to require manufacturers of digital devices to hardwire their products to respect copyright claims. Content providers have successfully invoked the DMCA to obtain orders preventing websites from linking to other websites that make available programs that could be used to circumvent copy protection." (footnotes omitted)); Borland, *supra* note 20.

71. *See Verizon III*, 351 F.3d at 1232.

72. *See In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24 (D.D.C. 2003), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003) [hereinafter *Verizon I*].

73. *See Verizon III*, 351 F.3d at 1232; *see also* Kreimer, *supra* note 20, at 23-24.

74. *See supra* Part II.

75. "The RIAA is a trade association representing record companies which create, manufacture and distribute most of the sound recordings produced and sold in the United States. In June 2003, the RIAA announced a nationwide effort to identify and sue individuals committing copyright infringement using P2P systems." *In re* Charter Commc'ns, Inc., 393 F.3d 771, 774 (8th Cir. 2005).

Services, through use of a Section 512 Subpoena.[76] Initially, Verizon refused to comply with the subpoena, on the grounds that it is only a Conduit ISP and that the requirement that a 512(c) Notice accompany the Section 512 Subpoena meant that such subpoenas are not effective as against Conduit ISPs.[77] In essence, Verizon argued that the purpose of a 512(c) Notice is to facilitate the removal of material from the Internet, something that Conduit ISPs such as Verizon are unable to do, and thus, Congress could not have intended that Section 512 Subpoenas apply to Conduit ISPs.[78] The District Court for the District of Columbia rejected Verizon's argument, and after continued proceedings, ultimately rejected all of Verizon's arguments, and directed it to comply with the RIAA's subpoena.[79]

On appeal, however, the Court of Appeals for the District of Columbia Circuit took a different view of Verizon's interpretation of the Section 512 Subpoena and the requirement of an accompanying 512(c) Notice.[80] The Court of Appeals placed great significance on the fact that a 512(c) Notice is enumerated under the Storage ISP function specific provisions.[81] It explained:

> Notably present in §§ 512(b)-(d), and notably absent from § 512(a), is the so-called notice and take-down provision. It makes a condition of the ISP's protection from liability for copyright infringement that "upon notification of claimed infringement as described in [§ 512](c)(3)," the ISP "responds expeditiously to remove, or disable access to, the material that is claimed to be

76. *See Verizon I*, 240 F. Supp. 2d at 45.

77. *Id.* After the district court rejected this argument, the RIAA served a second subpoena, and once again Verizon refused to comply, arguing this time that the district court lacked Article III jurisdiction to issue a subpoena with no underlying case or controversy pending before the court, and that § 512(h) violates the First Amendment, because it lacks sufficient safeguards to protect an Internet user's ability to speak and to associate anonymously. *See Verizon II*, 257 F. Supp. 2d at 247-48. While a full discussion of these arguments is beyond the scope of this article, a number of commentators have raised similar concerns regarding the possibilities for abuse of the Section 512 Subpoena. *See, e.g.*, DRATLER, *supra* note 45, § 6.05 ("Th[e section 512 subpoena] statutory scheme is thus a stark one. Clerks of the various United States district courts are to serve as a kind of 'vending machine' for subpoenas directed to service providers. In go the coins—a copy of the notification, a proposed subpoena, and a declaration—and out pops the signed subpoena, endowed with all the power and majesty of the judicial branch of the government of the United States. The requester need do little more than profess an intent not to misuse the subpoena. There is no explicit requirement of good faith; no review by any independent intelligence is required; and there is no provision for exercise of discretion. In go the coins, and out pops the subpoena, perhaps in the process depriving a person not yet shown to have infringed anything of valuable rights to privacy and anonymity.").

78. *Verizon I*, 240 F. Supp. 2d at 26.

79. *Id.* at 44-45.

80. *Verizon III*, 351 F.3d at 1237-39 .

81. *Id.*

infringing."[82]

The court then reasoned that the purpose of the 512(c) Notice is to trigger an obligation on the part of the receiving ISP to remove infringing material—an obligation a Conduit ISP cannot satisfy:

> Infringing material obtained or distributed via P2P file sharing is located in the computer (or in an off-line storage device, such as a compact disc) of an individual user. No matter what information the copyright owner may provide, the [Conduit] ISP can neither "remove" nor "disable access to" the infringing material because that material is not stored on the ISP's servers.[83]

Consequently, the court concluded that Section 512 Subpoenas cannot be issued to Conduit ISPs.

In essence, under the District of Columbia Circuit's interpretation of sub-section 512(c), a copyright holder cannot serve a *proper* 512(c) Notice on a Conduit ISP, because the copyright holder cannot provide information therein that will ultimately enable such an ISP to remove infringing material from the Internet (because Conduit ISPs are incapable of removing *any* material from the Internet).[84] Or, expressed from the perspective of a Conduit ISP, inasmuch as Conduit ISPs are unable to remove material from the Internet, it is impossible for any Conduit ISP to *comply* with a 512(c) Notice.[85] Thus, the *Verizon III* court's conclusion that Section 512 Subpoenas are not available in connection with Conduit ISPs, hinges on its reasoning that the service of a 512(c) Notice on an ISP, under any circumstances, *mandates the removal of infringing material from*

---

82. *Id.* at 1234 (citations omitted).

83. *Id.* at 1235. The court further found that a Conduit ISP's obligation under subsection 512(a) to "disable access" to the Internet under appropriate circumstances is not a substitute method of removing infringing material from the Internet. *Id.* The court found that the Act identifies removal of infringing material and disabling end-user access as two distinct remedies. *Id.* "These distinct statutory remedies establish that terminating a subscriber's account is not the same as removing or disabling access by others to the infringing material resident on the subscriber's computer." *Id.*

84. *See id.*

85. *See id.*; *see also In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 949 (M.D.N.C. 2005) ("[P]roviders discussed in subsections (b), (c), and (d) all engage in some form of information storage. These three subsections all contain a requirement that the providers respond to a written notification described in subsection (c)(3). The subsection (c)(3) notification, among other things, must be '"reasonably sufficient to permit the provider to locate the material"' so that the provider can remove or disable access to infringing information stored on the providers' systems. The notification in subsection (c)(3) presumes that the information is stored on a provider's system. . . ." (footnote and citation omitted)). These provisions cited by the court in *In re Subpoena* go toward locating the material, something that a conduit ISP would not be able to do, because the material is not stored. So the foregoing would not be helpful in locating the material.

the Internet.[86]

In *In re Charter Communications, Inc., Subpoena Enforcement Matter,*[87] the RIAA again attempted to obtain Internet subscriber identities from a Conduit ISP through use of a Section 512 Subpoena. Charter refused to comply with the subpoena, raising the same arguments previously raised by Verizon in its litigation with the RIAA, which were again rejected by the trial court.[88]

Just as occurred in *Verizon III*, however, the Court of Appeals for the Eight Circuit reversed.[89] The Eight Circuit also emphasized the reference to the 512(c) Notice in sub-section 512(h) and its absence from the Conduit ISP safe harbor provision set forth in sub-section 512(a).[90] Reviewing the analysis of the District of Columbia Circuit in *Verizon III*, the Court of Appeals adopted the *Verizon III* construction of sub-section 512(h) in toto:

> We agree with and adopt the reasoning of the United States Court of Appeals for the District of Columbia Circuit in *Verizon* [*III*] as it pertains to this statutory issue. Thus, because the parties do not dispute that Charter's function was limited to acting as a conduit for the allegedly copyright protected material, we agree § 512(h) does not authorize the subpoenas issued here. As a court we are bound to interpret the terms of the statute and not to contort the statute so as to cover the situation presented by this case.[91]

Finally, in *In re Subpoena to University of North Carolina at Chapel Hill*, the RIAA was again involved in litigation with a Conduit ISP regarding the right to obtain the identities of suspected infringers through use of Section 512 Subpoenas.[92] As in the foregoing cases, the RIAA learned of the infringing conduct by monitoring relevant Internet activity, but was able to obtain only the "cyber-pseudonyms" or screen names of the suspected infringers.[93] This information indicated that the suspected infringers each obtained Internet access through the University of North Carolina at Chapel Hill,[94] which ultimately decided to challenge the subpoenas

86. *Verizon III*, 351 F.3d at 1235.

87. 393 F.3d 771 (8th Cir. 2005).

88. *Id.* at 775.

89. *Id.* at 773.

90. *Id.* at 776 ("The absence of the remove-or-disable-access provision (and the concomitant notification provision) makes sense where an ISP merely acts as a conduit for infringing material—rather than directly storing, caching, or linking to infringing material—because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material.").

91. *Id.* at 777. Judge Diana E. Murphy vigorously dissented from the majority opinion. *See id.* 778-86 (Murphy, J., dissenting); discussion *infra* Part IV.

92. 367 F. Supp. 2d 945, 950 (M.D.N.C. 2005).

93. *Id.* at 946.

94. *Id.* ("[T]he RIAA was able to ascertain that [the alleged infringer] 'hulk'

served by the RIAA.[95] Although the District Court for the Middle District of North Carolina court expressed some concern as to whether its disposition was consistent with the purpose of the Liability Limitation Act, the court nonetheless followed the reasoning of *Verizon III* and *In re Charter* and quashed the Section 512 Subpoenas.[96]

As discussed in Part IV, while the *Verizon III* construction of sub-section 512(h) and its incorporation of the 512(c) Notice is plausible, it is not compelling.[97] There are alternative interpretations of the statutory language that are at least equally reasonable,[98] and

---

receives access to the internet through the University of North Carolina at Chapel Hill (UNC) and that [the alleged infringer] 'CadillacMan' receives internet service through North Carolina State University (N.C. State). As their internet service providers (ISPs), UNC and N.C. State should be aware of 'hulk' and 'CadillacMan's' true identities. For this reason, the RIAA obtained subpoenas from the Clerk of this Court directed to the schools pursuant to the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512. The subpoenas and their attachments identify copyright violations that the RIAA claims 'hulk' and 'CadillacMan' committed and seek to compel the schools to provide it with the alleged infringers' actual names, addresses, telephone numbers, and e-mail addresses." (citation omitted)).

95. *Id.* at 947.

96. *Id.* at 952-54. Most recently in July, 2007, the District Court for the Eastern District of Virginia became another adherent to the *Verizon III* construction of subsection 512(h). *See* Interscope Records v. DOES 1-7, 494 F. Supp. 2d 388, 390-91 (E.D. Va. 2008).

97. To be sure, the majority of the federal circuits have yet to accept that the *Verizon III* construction of subsection 512(h) casts concrete doubt on the applicability of Section 512 Subpoenas to Conduit ISPs. Indeed at least some courts, without deciding the specific issue, appear to be headed in the opposite direction. *See, e.g.*, Loud Records, LLC v. DOES 1-116, No. 3:04-CV-0771-N, 2005 U.S. Dist. LEXIS 2831, at *1-2 (S.D.N.Y. 2005) (specifically noting division of authorities regarding the right to serve identity disclosure subpoenas on Conduit ISPs); Elektra Entm't Group, Inc. v. DOES 1-9, No. 04 Civ. 2289, 2004 U.S. Dist. LEXIS 23560, at *9-13 (S.D.N.Y. 2004) (denying motion to quash subpoena to ISP, which motion was based on First Amendment right to speak anonymously).

98. For example, assuming the reference to the 512(c) Notice is in fact a directive that the receiving ISP remove material, it is not entirely clear why it would be insufficient for a Conduit ISP simply to respond that it lacks the capacity to do so. Indeed, subpoenas duces tecum are frequently served upon subpoenees who do not possess responsive documents, and a truthful statement to that effect usually does not result in a contempt citation. *See* HON. DAVID HITTNER ET AL., PRACTICE GUIDE: FEDERAL CIVIL PROCEDURE BEFORE TRIAL 11:1930 (5th Circuit ed. 2008) ("Production of Documents for Inspection: A party is obliged to produce all specified relevant and nonprivileged documents or other things which are in his or her "possession, custody or control" on the date and place specified in the request. . . . If there are no documents responsive to the request, the responding party need only say so in a certified response pursuant to Rule 26(g)."); *see also* 1 HOWARD B. ABRAMS, THE LAW OF COPYRIGHT § 5:163 (2008) ("Unless otherwise provided by section 512(h) or the relevant local court rules, the rules governing issuance of the subpoena and remedies for noncompliance with the subpoena shall be governed to the greatest extent possible by the provisions of the Federal Rules of Civil Procedure concerning the issuance, service and

more important, that preserve the stated purpose of the Liability Limitation Act.[99] Thus, it is possible to construe the Section 512 Subpoena provision so as to include Conduit ISPs within its reach, and thereby maintain the balance of copyright holder/ISP/subscriber interests the Act was intended to achieve. In light of the purpose of the Act, such viable, alternative constructions of sub-section 512(h) should be adopted by those courts that have yet to decide this issue.

IV. CONGRESSIONAL PRIORITIZATION OF COPYRIGHT PROTECTION OVER INTERNET "CYBER-PSEUDONYM" PRIVACY

As with all questions of statutory construction, determining whether Section 512 Subpoenas are effective against Conduit ISPs involves a two step analysis: first, asking what did Congress say? and second, determining what did Congress intend? One begins by parsing the literal language of the statute, and then, to the extent that that language is ambiguous, divining Congress's specific objectives through review of the statute's legislative history, assessed

---

enforcement of a subpoena duces tecum."). Moreover, certainly there are instances in which a Storage ISP receives a 512(c) Notice in connection with material that is no longer on the Internet, and in such a case, said Storage ISP has no more capability to remove infringing material than would a Conduit ISP. For a similar argument, see Zach Chaffee-McClure, *Train in Vain: The Clash Between the RIAA and the Eighth Circuit Over Whether the DMCA Subpoena Provisions Applies to Peer-to-Peer Networks, and the Need to Steer the DMCA Back on Track with Congressional Intent,* 45 WASHBURN L.J. 175, 191 (2005) ("When a court issues a subpoena to a conduit ISP, there simply is no material 'that is to be removed or access to which is to be disabled.' Section 512(c)(3)(A)(iii) does not demand that a copyright holder identify any material at all, unless that material 'is to be removed or access to [it] is to be disabled.' If there is no material to identify, as is the case when a court issues a subpoena to a conduit ISP, then the RIAA can hardly fail to identify it." (footnotes omitted)); Trevor A. Dutcher, *A Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, As Applied in* RIAA v. Verizon Internet Services, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 493, 512 (2005) ("This would be no different than the case where a s 512(c)-type user storing files on his ISP's 'web storage' deletes the files after he is discovered by the copyright holder, but before the subpoena is served upon the ISP. In that case, the ISP would once again be unable to 'locate' the infringing material and the subpoena would simply be unenforceable, for a failure to provide proper notice under § 512(c)(3)(A)(iii); but certainly nobody would argue that the subpoena power simply does not apply to a situation covered by § 512(c) because the risk of being unable to locate the files exists.").

99. The legislative history to the Act would also seem to support this perspective. *See* H.R. REP. NO. 105-551, pt. 2, at 61 (1998) ("The Committee intends that an order for disclosure be interpreted as requiring disclosure of information in the possession of the service provider, rather than obliging the service provider to conduct searches for information that is available from other systems or networks.") For an argument that for reasons of efficiency, Congress simply chose to reference 512(c) in subsection 512(h) rather than draft an entirely new notice provision, see Dutcher, *supra* note 98, at 510-11.

in the context of copyright social policy as a whole.[100] Ad-hoc judgments, however, as to how Congress might or should have acted, must be avoided.[101] Even if Congress has failed to pursue what in retrospect appears to be the optimum course, if the adopted course is within Congressional discretion, it must be accepted by the courts.

A. The Provisions of Subsection 512(h) are Unambiguous

1. The Literal Text of Subsection 512(h) Anticipates Application to Conduit ISPs

In ascertaining whether Congress intended that Section 512 Subpoenas be effective against Conduit ISPs, it is necessary to first determine whether the requirement in sub-section 512(h)(2)(A), that a 512(c) Notice accompany the Subpoena, renders the overall mandate of sub-section 512(h) ambiguous. If not, and the language and intent of the statute are reasonably clear, then its directives should not be evaded by the creation of a false ambiguity in construing its terms.[102]

---

100. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 775 (8th Cir. 2005) ("We begin our analysis with the language of the statute itself." (citing U. S. Sec. & Exch. Comm'n v. Zahareas, 272 F.3d 1102, 1106 (8th Cir. 2001)); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 951 (M.D.N.C. 2005) ("In determining whether the [subsection 512] subpoenas in this case were authorized by the DMCA, the Court begins by looking at the language of the statute itself in order to determine whether its meaning is plain and unambiguous. In making this determination, the Court should be guided by the context surrounding the language in question, along with the broader context of the statute as a whole." (citation omitted)).

101. *In re Subpoena*, 367 F. Supp. 2d at 953-54; *see also* Mikel R. Boeve, Note, *Will Internet Service Providers Be Forced to Turn in Their Copyright Infringing Customers? The Power of the Digital Millennium Copyright Act's Subpoena Provision After In re* Charter Communications, 29 HAMLINE L. REV. 115, 134 (2006) ("When courts are asked to interpret the meaning and scope of a statute they look to various legal precedents to guide them. When interpreting a statute, most courts start with the specific language of that statute. If this language is ambiguous, then courts likely will consider the congressional intent behind the statute's enactment. Courts also view statutory construction 'as a holistic endeavor' that should at least take into account the statute's text in its entirety, along with structure, punctuation, and subject matter. Furthermore, interpretations by the courts that leave portions of a statute 'superfluous' should be avoided." (footnotes omitted)).

102. *See* 73 AM. JUR. 2D *Statutes* § 75 (2007) ("In some instances, the purpose of a statute is expressly stated therein. Where such declared purpose is not incompatible with the meaning and effect of the statute, it is to be taken as true. Or, as sometimes stated, the "plain purpose" of legislation is determined in the first instance with reference to the plain language of the statute itself. A court will look to the statutory text to determine the purpose of a statute because the purpose of an enactment is embedded in its words, even though the purpose is not always pedantically expressed in words. . . . The rule permitting departure from the literal meaning of a statute has no application where the literal meaning appears to be consonant with the purpose of

On its face, sub-section 512(h)(2)(A)'s requirement that a 512(c) Notice accompany a Section 512 Subpoena does not render the statute ambiguous. The undisputed purpose of sub-section 512(h) is to provide a procedure through which the identities of alleged infringers can be obtained by subpoena. The requirement that a 512(c) Notice accompany the Subpoena does not contradict this stated purpose. The reference to a 512(c) Notice does not include any directive that the receiving ISP undertake any inconsistent action upon receiving the Notice, that is, that the ISP act to remove infringing material from the Internet.[103] Indeed, whereas subsection 512(h) expressly directs that the receiving ISP must comply with the Section 512 Subpoena by providing the information requested therein, it does *not* specify what, if anything, the ISP must do in response the 512(c) Notice.[104]

In point of fact, sub-section 512(h)(2)(A) actually calls only for the provision of a notification as *described* in sub-section 512(c)(3)(A), as opposed to a notification *effective* under that sub-section.[105] The *Verizon III* appellate court overlooks this difference in the wording of the two sub-sections, and mistakenly quotes sub-section 512(h) as requiring a notification "effective" under 512(c).[106] The importance of this distinction[107] is that the 512(c) Notice referred to in sub-section

---

the statute." (footnotes omitted)).

103. Such action would be "inconsistent" for a Conduit ISP, given its inability to "take-down" infringing material. As discussed below, however, such a directive by subsection 512(h) was *inferred* by certain courts, which assumed that a 512(c) Notice serves the same function under subsection 512(h) as it does under subsection 512(c). While such an inference is reasonable, it is not inevitable, and when considered in the context of the statute as a whole, it is counter-intuitive, if not outright illogical.

104. *See* 17 U.S.C. § 512(h) (2006).

105. *Compare* § 512(c)(A), *with* § 512(h)(2).

106. *Verizon III*, 351 F.3d at 1236.

107. Concededly, subsection 512(h)(4) employs yet *another* term, and calls for a notification that "satisfies" 512(c)(3)(A), a term which seems to fall somewhere in between "effective" and "described." Realistically, a notice that meets the description set forth under 512(c)(3)(A) will likely also "satisfy" as well as be "effective" under that subsection. The use of the word "effective" in 512(c)(3)(A), however, suggests that in the context of *that* subsection, the role of the 512(c) Notice is to distinguish those notices which an ISP might receive that are insufficient to trigger the obligation of a response (for example, a notice which fails to accurately describe the allegedly infringing material) from those notices that are sufficient to trigger such an obligation (and therefore implicate the ISP's safe harbor immunity). As discussed below, however, subsection 512(h) does not import the language of 512(c) in its entirety, and is not concerned with establishing the prerequisites to ISP safe harbor immunity. Rather, 512(h) is intended to set forth a framework in which subpoenas might be issued and subscriber identities disclosed. Finally, specifically insofar as Conduit ISPs are concerned, subsection 512(a) obviously makes no reference to a 512 Notice as a condition to safe harbor immunity. Thus, unlike the situation with respect to subsections 512(b) and (d), which at least reference the 512(c) Notice, there is no

512(h)(2)(A) is not necessarily intended to trigger the broader sub-section 512(c) Storage ISP obligation to "respond[] expeditiously" to the Notice, that is, the obligation to "take-down" infringing material (in order to preserve any applicable Storage ISP safe harbor immunity).[108] In short, given that there is no express directive within the language of sub-section 512(h) that a receiving ISP respond to the Notice and remove infringing material from the Internet, the literal language of sub-section 512(h)(2)(A) does not impose any compliance obligations that Conduit ISPs are unable to perform.[109]

---

reason to construe 512(h) to require a response (i.e., a "take-down") to the 512 Notice and create the untenable paradox for Conduit ISPs envisioned by the *Verizon III* appellate court.

108. *See* § 512(c)(1)(C). The alternative interpretation offered herein seems even more compelling when one considers the "function specific" nature of the various safe harbor provisions, and the fact that subsection 512(c) specifically identifies removal of infringing material from the Internet as a condition of Storage ISP immunity. *See id.* That entire provision, however, was not imported into the 512(h)(2)(A) reference to the 512(c) Notice. In her dissent in *In re Charter*, Judge Diana E. Murphy makes a related observation, specifically, that the express language of the Act does not exclude Conduit ISPs from the reach of a Section 512 Subpoena. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 778-86 (8th Cir. 2005) (Murphy, J., dissenting) ("The subpoena power created by Congress in § 512(h) does not limit the type of service provider for whom subpoenas may be issued in the fight against internet piracy. . . . Although Charter contends that the subpoena power in the DMCA is limited by the function of the ISP, such a limitation is not to be found in a plain reading of the DMCA. To the contrary, the statute defines 'service providers' in § 512(k) as all 'providers of online services or network access,' including conduit providers who offer the 'transmission . . . of material of the user's choosing, without modification.' If Congress had wanted to limit the type of ISP subject to a statutory subpoena, it could have easily specified that in § 512(h), but it did not. In the absence of such a limitation, the statute's definition of 'service provider' in § 512(k)(1) controls . . . ." (second alteration in original) (citation omitted)); *see also* Chaffee-McClure, *supra* note 98, at 189-90 ("The subpoena provision itself places no restrictions on the type of ISP to which a court may issue a subpoena. Moreover, in creating an implicit restriction on the type of ISP subject to the subpoena power, the Eighth Circuit misread the notification provision to demand that . . . the ISP store the infringing material. The notification provision requires neither that the ISP be able to locate the infringing data nor that the ISP be able to remove the infringing data.").

109. For an argument that a Conduit ISP can at least *locate* infringing material, see Chaffee-McClure, *supra* note 98, at 196 ("There are multiple ways that a conduit ISP can locate infringing material that resides on an Internet user's computer. First, an ISP can locate the infringing material in the same manner that the copyright holder can discover the material. When a user shares a file on a P2P network, any party who wishes to download that file must first locate it. In *In re Charter*, the RIAA used a tracking program to detect copyrighted files on P2P networks. The RIAA also downloaded the suspect files. A conduit ISP may use one or both of the same techniques, or some technological equivalent, to locate files on a subscriber's computer. Second, to comply with a subpoena, an ISP must locate the infringing data because the ISP must identify which customer corresponds to the suspect IP address. 'Only the ISP . . . can link a particular IP address with an individual's name and physical address.' Thus, an ISP can locate the material with greater specificity than any other party by

In addition to the literal wording of sub-section 512(h)(2)(A), the express language of sub-section 512(h)(5) affirmatively clarifies that there is no requirement that an ISP respond to the 512(c) Notice which must accompany a Section 512 Subpoena:

> Upon receipt of the issued subpoena . . . the service provider shall expeditiously disclose to the copyright holder . . . the information required by the subpoena, notwithstanding any other provision of law *and regardless of whether the service provider responds to the [512(c)] notification.*[110]

Thus, in accordance with sub-section 512(h)(5), *even a Storage ISP* could ignore the accompanying 512(c) Notice and fail to remove infringing material from the Internet, without risking judicial sanction for failure to comply with the Subpoena.[111]

Obviously, most Storage ISPs will almost certainly act to remove infringing material from the Internet upon receiving a 512(c) Notice, whether the Notice is served independently or in conjunction with a Section 512 Subpoena, because of its importance to Storage ISP safe harbor immunity.[112] On the other hand, the 512(a) safe harbor for Conduit ISPs has no 512(c) Notice reference whatsoever, and thus is not dependent upon any removal of infringing material. Thus, a Conduit ISP that receives a Section 512 Subpoena with accompanying 512(c) Notice need only be concerned with the express directives of sub-section 512(h) and not fear the loss of its immunity for failure to remove infringing material from the Internet.

---

identifying the Internet user that stores the infringing data. In this case, Charter complied with the subpoenas, thereby demonstrating the ability to locate subscribers. Charter erred in assuming that a conduit ISP cannot locate infringing material that resides on a user's computer." (alteration in original) (footnotes omitted) (quoting *In re Charter*, 393 F.3d at 773); *see also* Dutcher, *supra* note 98, at 502-03 (making a similar argument).

110. § 512(h)(5) (emphasis added).

111. Of course, although the failure to respond to a 512(c) Notice carries no penalty under subsection 512(h), disregard of the 512(c) Notice would imperil a Storage ISP's safe harbor immunity. So long as the ISP (whether Conduit or Storage) has disclosed the identities requested by the Section 512 Subpoena, however, any failure to remove infringing material does not affect its status under subsection 512(h). Professor Nimmer appears to be of the same view. *See* 3 NIMMER ON COPYRIGHT § 12B.09[A] (2008) ("[E]ven if the service provider chooses not to [respond to the 512(c) Notice and] disable access to the subject material and to defend its decision on a basis other than Section 512, it must still turn over the requested information [in response to the Section 512 Subpoena]." (footnotes omitted)).

112. *See In re Charter*, 393 F.3d at 776 ("[A] specific purpose of the notification provision is to allow an ISP, after notification, the opportunity to remove or disable access to infringing material and thereby protect itself from liability for copyright infringement. Therefore, as one might expect, each safe harbor which covers an ISP function allowing the ISP to remove or disable access to infringing material (i.e., the storage, caching, and linking functions) refers to the notification provision *and* contains a remove-or-disable-access provision.").

In the absence of sub-section 512(h)(5), the requirement that a 512(c) Notice accompany a Section 512 Subpoena might arguably render 512(h) ambiguous, in that it could be reasonably interpreted to require that the receiving ISP take *some* action in response to the Notice, as part of its compliance with the Subpoena. Moreover, as reasoned by the *Verizon III* court, such an obligation would thereby necessitate that the Section 512 Subpoena be held inapplicable to Conduit ISPs, because such ISPs could never comply fully with the Subpoena's mandates.[113] The express language of sub-sections 512(h)(2) and (5), however, eschew such a Gordian contradiction. Thus, there is no facial inconsistency or ambiguity created by the reference to the 512(c) Notice in the provisions of sub-section 512(h)(2)(A).

2. Applying Section 512 Subpoenas to Conduit ISPs Implements the Legislative Purpose of Subsection 512(h)

In some situations, a specific statutory phrase or provision, although independently unambiguous, can nonetheless create an overall ambiguity when considered in the context of the purpose of the statute as a whole.[114] Thus, while the literal reference in sub-section 512(h)(2)(A) to the 512(c) Notice does not create any express compliance (i.e., take-down) obligations on the part of the receiving ISP, there remains the question as to whether the mere reference to the 512(c) Notice is somehow inherently antithetical to the overarching purpose of sub-section 512(h), and thus creates an internal inconsistency within the statute.

The purpose of sub-section 512(h) is to set forth a procedure whereby the identities of alleged infringers might be obtained from an ISP, without the need for copyright litigation or extensive discovery.[115] Accordingly, the requirement that a 512(c) Notice accompany a Section 512 Subpoena should be assessed for its impact on this procedure.[116]

---

113. *See Verizon III*, 351 F.3d at 1236.

114. *See, e.g.*, Richards v. United States, 369 U.S. 1, 11 (1962) ("[A] section of a statute should not be read in isolation from the context of the whole Act, and that in . . . interpreting legislation, [the Supreme Court] 'must not be guided by a single sentence or member of a sentence, but [should] look to the provisions of the whole law and to its object and policy.'" (footnote omitted)); *see also* Davis v. Mich. Dep't of Treasury, 489 U.S. 803, 809 (1989) (It is a "fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme.").

115. § 512(h).

116. *See* United States v. Pub. Utils. Comm'n of Cal., 345 U.S. 295, 315 (1953) ("Where the language and purpose of questioned statute is clear," courts "follow the legislative direction in interpretation," but "where words are ambiguous" or would

In serving a Section 512 Subpoena, the copyright holder is seeking the identity of an alleged infringer. The provision of a 512(c) Notice to an ISP, however, actually supports this objective. First, the information called for in the 512(c) Notice is useful in confirming that the party serving the Section 512 Subpoena has a legitimate basis for seeking the identities of the ISP's subscribers.[117] The information sets forth the party's legal interest as a copyright holder and, by detailing specific occasions of unauthorized use of copyrighted material, the Notice confirms that the copyright holder is engaged in more than a mere fishing expedition. In addition, the 512(c) Notice information can also be helpful in pinpointing the conduct at issue and/or identifying the person who actually engaged in that conduct. For example, where the alleged infringer is unaware that her conduct impinges upon the rights of a copyright holder, or where she allows other users access to her computer, a reference to specific material or dates of dissemination will be more meaningful than a generic accusation of infringement.[118] Thus, the incorporation of a 512(c)

---

bring about an end completely at variance with the purpose of statute if literally construed "the judiciary may properly use legislative history to reach a conclusion.").

117. In her dissent in *In re Charter*, Judge Murphy offers additional reasons as to why Congress intended that the 512(c) Notice be used to aid in identifying suspected infringers (as opposed to effectuating the take-down of infringing material) when the notice accompanies a Section 512 Subpoena. *See In re Charter*, 393 F.3d at 778-80 (Murphy, J., dissenting). She wrote that:

> The majority claims that [the language in subsection 512(c)(3)(A)] excludes conduit ISPs, but the language does not say that. The subsection defines the material to be identified in two ways: (1) material that is "claimed to be infringing" and (2) material that is "the subject of infringing activity and that is to be removed or access to which is to be disabled."
>
> . . . .
>
> The distinction within § 512(c)(3)(A) between material "claimed to be infringing" and material that is "the subject of infringing activity and that is to be removed or access to which is to be disabled" appears to carry forward the initial distinction in the DMCA between § 512(a) conduit ISPs and §§ 512(b)-(d) storage ISPs. The copyrighted material stored on an ISP's network becomes the subject of infringing activity when it is unlawfully duplicated by subscribers. In order to remove such material or disable access to it, a storage ISP needs it to be identified. On the other hand, when a subscriber transfers copyrighted material through a conduit ISP, that service provider cannot remove the material from the network. It can, however, provide identifying information about the offeror of the material "claimed to be infringing."

Id. at 781.

118. *See, e.g.*, *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005) ("[T]here is no doubt that the notification document contains valuable and necessary information in order for a subpoena to be issued. Without the contents of the notification, there would not be a basis for the subpoena, except for a conclusory allegation that the subpoena is sought to obtain the identity of an alleged

Notice reference into the provisions of sub-section 512(h)(2)(A) actually furthers the overarching purpose sub-section 512(h), and therefore does not create any substantive inconsistency or ambiguity within the statute.

Moreover, when a copyright holder serves a Section 512 Subpoena, she is *not* seeking the removal of the infringing material from the Internet. As provided in sub-sections 512(b) through (d), the copyright holder does not need to serve a Section 512 Subpoena in order to obtain this remedy. A copyright holder can trigger a Storage ISP's take-down obligation merely by serving a "stand-alone" 512(c) Notice, without attaching it to a Section 512 Subpoena. In short, while a Storage ISP may have good reason to respond to a 512(c) Notice, that impetus is simply irrelevant to its compliance with a Section 512 Subpoena.[119]

The construction of sub-section 512(h) proffered by the *Verizon III* court and its progeny creates an *artificial* statutory ambiguity, in part because the *Verizon III* construction improperly superimposes the *full text* and express objectives of sub-section 512(c) (as opposed to only the narrower text and limited objectives of sub-section 512(c)(3)) onto the terms and provisions of sub-section 512(h). While sub-section 512(h) makes a paraphrased reference to 512(c)(3), it does not incorporate verbatim sub-section 512(c) in its entirety. This is an important point because sub-section 512(c) *as a whole* is concerned with the eligibility of certain Storage ISPs for a specific kind of safe harbor immunity. Where a Storage ISP's activities meet the definition of service provider set forth in 512(c), and said ISP has complied with all of sub-section 512(c)'s affirmative requirements, it is entitled to the safe harbor immunity. On the other hand, 512(c)(3) does not set forth a prerequisite to safe harbor immunity, but rather delineates a situation under which a Storage ISP may *forfeit* its immunity by failing to provide an "expeditious response" to a proper 512(c) Notice.[120] Moreover, if the copyright holder's attempt to serve

infringer. Thus, notification information is a crucial part of the subpoena process." (citation omitted)). Indeed, when confronted with the information contained in the 512(c) Notice, some unintentional infringers will likely accept responsibility, thereby expediting resolution of the matter.

119. The reasoning of the *Verizon III* appellate court and similar courts that a copyright holder might use the Section 512 Subpoena to demand that a Conduit ISP remove material from the Internet is circular in this regard. Inasmuch as neither 512(a) nor 512(h) expressly requires Conduit ISPs to remove material, there is no threat that copyright holders could so misuse the Section 512 Subpoena unless the courts first read such a mandate into the terms of 512(h). Moreover, if a copyright holder did attempt to so misuse the Section 512(c) Subpoena, the receiving Conduit ISP could simply respond that it lacks the capacity to remove the subject material from the Internet, in order to avoid a contempt sanction for noncompliance.

120. This risk of forfeiture arises only where a *proper* 512(c) Notice has been served,

a 512(c) Notice fails to satisfy the precise requirements of sub-section 512(c)(3), the Storage ISP's safe harbor immunity status is unaffected—a Storage ISP is not required to respond (expeditiously or otherwise) to a defective Notice.

Accordingly, when a Storage ISP receives both a Section 512 Subpoena and a proper 512(c) Notice, and elects to take down any pertinent infringing material, but declines to identify the alleged infringer, its eligibility for the safe harbor immunity will remain intact; the disclosure of subscriber identities is not a condition of ISP immunity.[121] In such a case, the ISP's only concern is a possible citation for contempt as a result of its failure to comply with the directives of the Section 512 Subpoena.[122] Of course, none of the "take-down" directives appear in the Conduit ISP safe harbor provision, and thus the issue is irrelevant to Conduit ISPs, their safe harbor immunity, or their compliance with a Section 512 Subpoena.

In sum, the mandatory reference in sub-section 512(h)(2)(A) to the 512(c) Notice does not conflict with the overarching purpose of establishing an expeditious mechanism for the disclosure of subscriber identities. In fact, given that the requirement that a 512(c) Notice accompany a Section 512 Subpoena actually *supports* the overall objective of sub-section 512(h), any purported conflict or ambiguity in the statute's terms is artificial at best.[123] Construing

---

whereupon an otherwise qualifying Storage ISP can lose its immunity if it subsequently fails to remove infringing material from the Internet. *See* § 512(c)(1)(C).

121. *See* § 512(c). By the same token, the ISP could disclose subscriber identities but refuse to remove the infringing material, which would only affect its eligibility for Storage ISP immunity. *See* S. REP. NO. 105-190, at 45 (1998) ("On the other hand, the service provider is free to refuse to 'take down' the material or site, even after receiving a notification of claimed infringement from the copyright owner; in such a situation, the service provider's liability, if any, will be decided without reference to new Section 512(c).").

122. Professor Dratler makes the same observation. *See* DRATLER, *supra* note 45, § 6.05[2][c]; *see also* Dutcher, *supra* note 98, at 509 ("The safe harbors are concerned with providing shelter for ISPs from secondary liability arising from the acts of their subscribers. The subpoena power, on the other hand, gives plaintiffs a mechanism to identify and seek a remedy against direct infringers. These are separate tools. An ISP may very well receive notice of an allegedly infringing use that is sufficient for a subpoena to issue; but whether the ISP actually acts upon that notice by "taking down" the material in order to avail itself of the safe harbor is a wholly separate issue and should have no bearing on the subpoena analysis.").

123. Judge Murphy makes a similar observation in her dissent in *In re Charter*. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 778-90 (8th Cir. 2005) (Murphy, J., dissenting). There, she wrote:

> Section 512(h), which creates the subpoena power, only references § 512(c)(3)(A) to indicate the kind of information which needs to be given to the clerk to request a subpoena. By referencing the elements of the notification in § 512(c)(3)(A), Congress avoided the necessity of repeating such notice details in § 512(h). The statutory requirement that storage service providers

the language of sub-section 512(h) to require the removal of infringing material is not only unnecessary, but unreasonable, at least with respect to Conduit ISPs, as it undermines the overarching purpose of 512(h).[124] Rather, construing the 512(c) Notice requirement to be consonant with the subpoena procedure function of sub-section 512(h) is the analytically sounder course. [125]

> expeditiously remove or disable access to infringing materials in order to avoid secondary liability is not rooted in this notification provision, but rather in those sections of the DMCA which set out the obligations of storage providers.

Id. at 781 (citations omitted); *see also* Boeve, *supra* note 101, at 138 ("The specifics of subsection (c)(3)(A) could have just been reproduced in section (h), but to avoid repetition and unduly long provisions a simple reference to subsection (c)(3)(A) was included instead. Some courts, however, have read too much into this reference back to subsection (c)(3)(A) and have concluded that the subpoena provision only applies to service providers that engage in storing data for their customers." (footnote omitted)).

124. Although both the present argument and the *Verizon III* construction of 512(h) are reasonable (at least with respect to Storage ISPs because of their independent obligation to remove infringing material from the Internet), a construction that 512(h) does not mandate a "take-down" is the most logical because of the differing objectives of the two subsections: providing immunity under 512(c) versus facilitating identity disclosure under 512(h). Finally, if there is some material ambiguity in subsection 512(h) making it necessary to look beyond its provisions for a context in which to construe its reference to the 512(c) Notice where the applicability of the 512 Subpoena to Conduit ISPs is the issue, it is at least equally reasonable, if not imminently logical, to look to 512(a) (as opposed to 512(c)) for context. While 512(a) does not discuss "take-down," it does state that Conduit ISPs remain amenable to limited injunctive relief—specifically, an injunction prohibiting them from providing service to repeat infringers. Both the 512(h) Subpoena and the 512(c) Notice are relevant to such injunctive relief. It would be necessary that a court have the identities of the alleged infringers in order to fashion an appropriate injunction, and the 512(h) Subpoena is the only express mechanism in the Act through which this information can be obtained.

125. Indeed, the argument that subsection 512(h) requires a "take-down" in response to the accompanying 512(c) Notice is no more compelling when considered in connection with Storage ISPs. Requiring a 512(c) Notice "take-down" in order to preserve a Storage ISP's immunity, but omitting this requirement from said ISP's compliance with a 512 Subpoena makes sense because of the differing purposes of the Storage ISP immunity provisions and the purpose of the Section 512 Subpoena. Under 512(b), (c), and (d), a Storage ISP can preserve its safe harbor immunity without disclosing the identity of alleged infringers. At the same time, the ISP can disclose subscriber identities in compliance with a 512 Subpoena, but nonetheless forfeit its immunity, if it fails to remove infringing material in response to a 512 Notice. When a Storage ISP receives *both* a 512(c) Notice and a Section 512 Subpoena, it risks the loss of safe harbor immunity *and* a citation for contempt depending upon what action it takes in response to the separate obligations created by the copyright holder's provision of these two documents. Thus, even with respect to Storage ISPs, there is no need to construe subsection 512(h) as mandating a "take-down" of infringing material.

3. Construing Subsection 512(h) to be Applicable to Conduit ISPs is Consistent with the Express Language of Complementary 512 Subsections

Finally, the express language of certain complementary sub-sections of section 512 further supports the analysis that subsection 512(h) should be construed as applicable to Conduit ISPs. [126] First, sub-section 512(a) states that Conduit ISPs entitled to its safe harbor immunity remain vulnerable to injunctive relief in favor of copyright holders. Subsection 512(j)(1)(B) clarifies that the injunctive relief available against Conduit ISPs is that of an order restraining such ISPs from providing Internet access service to repeat infringers. If Congress did not intend to apply 512 Subpoenas to Conduit ISPs, the injunctive relief provisions of sub-sections 512(a) and (j) become somewhat ethereal. In order to obtain an injunctive order against a specific subscriber, a copyright holder obviously must know the subscriber's identity. [127] It seems incongruous then that Congress would make this remedy available in connection with Conduit ISPs, but then exclude it from the reach of the Section 512 Subpoena, the precise mechanism through which copyright holders may most expeditiously obtain subscribers' names. [128]

In addition, sub-section 512(n) states that each type of safe harbor immunity is separate and distinct. [129] Whether an ISP can assert immunity under one sub-section (for example, whether a

126. 73 AM. JUR. 2D *Statutes* § 103 (2007) ("Sections and acts in pari materia, and all parts thereof, should be construed together and compared with each other. Because the object of the rule is to ascertain and carry into effect the legislative intent, it proceeds upon the supposition that the several statutes were governed by one spirit and policy, and were intended to be consistent and harmonious in their several parts and provisions. Under this rule, each statute or section is construed in the light of, with reference to, or in connection with, other statutes or sections." (footnotes omitted)); *see also* Kokoszka v. Belford, 417 U.S. 642, 650 (1974) ("When 'interpreting a statute, the court will not look merely to a particular clause in which general words may be used, but will take in connection with it the whole statute (or statutes on same subject) and objects and policy of the law, as indicated by its various provisions, and give to it such a construction as will carry into the execution the will of the legislature . . . .'" (quoting Brown v. Duchesne, 61 U.S. (19 How.) 183, 194 (1857))).

127. Indeed, § 512(j)(1)(B)(i) unsurprisingly requires that the subscriber be "identified in the order" restraining the ISP from providing Internet service. *See* 17 U.S.C. § 512(j)(1)(B)(i) (2006).

128. Granted, copyright holders can still obtain such injunctive relief by instigating litigation against a Conduit ISP, but this result obviously contradicts the spirit of the Liability Limitation Act as a whole. The idea is to *avoid* litigation against ISPs as a means by which to combat subscriber infringement. Thus, it does not seem logical that Congress would intend that copyright holders sue Conduit ISPs solely to obtain the identities of alleged infringers, rather than invoke the Section 512 Subpoena procedure.

129. *See* § 512(n).

Storage ISP "expeditiously responded" to a proper 512(c) Notice) is not dispositive as to its eligibility for safe harbor immunity under another sub-section (whether the ISP's service activity meets the definition of a Conduit ISP under sub-section 512(a)). Thus, whereas the failure to "take-down" infringing material in response to a 512(c) Notice will imperil a Storage ISP's safe harbor immunity under sub-sections 512(b), (c), and (d), it has no effect upon a Conduit ISP's eligibility for safe harbor immunity under sub-section 512(a). The *Verizon III* construction of sub-section 512(h), however, creates a link between Conduit ISP safe harbor immunity and infringing material "take-downs" that does not appear in the statute, and moreover, is inconsistent with the mandate of sub-section 512(n).[130]

Finally, insofar as sub-section 512(h) is not at all concerned with "function specific" ISP safe harbor immunity, it seems a stretch to conclude that Congress intended that sub-section 512(h) be construed to apply indirectly a condition of Storage ISP safe harbor immunity to Conduit ISPs, or worse, to serve as a means by which to immunize Conduit ISPs from both Section 512 Subpoenas and also the obligation to comply meaningfully with sub-section 512(j). Given the express directives of sub-section 512(n), it would seem that any doubts with respect to Congress's intentions in this regard should be resolved *against* applying the "take-down" function of a 512(c) Notice to Conduit ISPs, and especially against utilizing the "take-down" function as a means by which to exclude Conduit ISPs from the reach of Section 512 Subpoenas.

B. Even if the Language of 512(h) is Ambiguous, Construing 512(h) as Applicable to Conduit ISPs is the Most Reasonable Construction of the Statute

The argument that sub-section 512(h) unambiguously provides for the application of Section 512 Subpoenas to Conduit ISPs seems compelling. Concededly, however, reasonable arguments can be made that the language of 512(h) is not entirely free from ambiguity. Nonetheless, even if the language of sub-section 512(h) is indeed ambiguous, resolving such ambiguity to conclude that Section 512 Subpoenas are not effective against Conduit ISPs is not a reasonable construction of the statute. This is because (i) such a construction defeats the overall purpose of the Liability Limitation Act, that is, to preserve the rights of copyright holders while limiting the legal impact of ISP subscriber infringement upon ISPs, and (ii) an alternative, and at least equally plausible construction of the statute which would effectuate the legislative intent is available, and therefore should be adopted over a construction that would defeat the

130. *Verizon III*, 351 F.3d at 1237.

legislative goals. [131]

1. Arresting Internet Copyright Infringement is a Principal Goal of the Liability Limitation Act

There is no dispute that the problem of unauthorized Internet dissemination of copyrighted material continues to be one of the most important forms of copyright infringement today. "Approximately 90% of the content on peer-to-peer (P2P) systems is copyrighted movies, software, images, and music disseminated without authorization. It is estimated that more than 2.6 billion allegedly infringing music files are downloaded monthly."[132]

Since the passage of the DMCA, copyright holders have increasingly pursued litigation against individual infringers, to stem the tide of Internet copyright infringement.[133] The advent of P2P

---

131. If ambiguous language in a statute can be reasonably construed to effectuate the statute's purpose, then such a construction of the statute should be favored over alternative constructions at odds with the statutory objectives. *See* 73 AM. JUR. 2D *Statutes* § 75 (2007) ("In the interpretation of a statute of ambiguous terminology, the proper course is to adopt that sense of the words which promotes in the fullest manner the object of the statute. The general rule is that the words of a statute should receive their ordinary acceptation and significance, where such construction is consonant, and not at variance, with the purpose of the statute, and does not thwart or defeat the same, or where it is not obvious from the statute that the evil to be suppressed, or the remedy to be advanced, requires that the construction be limited or enlarged." (footnotes omitted)).

132. *In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773 (8th Cir. 2005); Elektra Entm't Group, Inc. v. DOES 1-9, No. 04 Civ. 2289, 2004 U.S. Dist. LEXIS 23560, at *2-3 (S.D.N.Y. 2004) ("A P2P network is an online media distribution system that allows users to have their computers function as an interactive Internet site, disseminating files for other users to copy. . . . The plaintiffs allege that they have found each of the defendants openly disseminating sound recordings whose copyrights they own on the P2P network. Plaintiffs themselves logged on to the P2P network and viewed the files that each defendant was offering to other users. According to plaintiffs, each defendant has chosen to make available from his or her computer hundreds of sound recordings whose copyrights are owned by various of the plaintiffs.") *See generally* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1099 (9th Cir. 2002); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001); Boeve, *supra* note 101, at 127 ("In March 2005, 26 million songs were purchased and downloaded legally from online stores while a total of 243 million songs in the same month were downloaded, mainly illegally, using peer-to-peer software. The public conception of illegal downloading may be viewed 'by some as an innocuous form of entertainment'; however, the economic truth behind the activity is that it results in substantial revenue losses for recording companies and for artists." (footnote omitted)); Ryan C. Edwards, *Who Said Nothing in This World is Free?* A&M Records, Inc. v. Napster, Inc.*: Problems Presented, Solutions Explored, and Answers Posed*, 89 KY. L.J. 835, 835 (2001).

133. *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 949-50 (M.D.N.C. 2005) ("As a consequence of the new [P2P] technology, litigation initiated by copyright holders now targets individuals, as opposed to internet service providers or bulletin board operators. In order to pursue such alleged infringers, the [copyright

technology, however, has facilitated anonymous Internet misconduct.[134]

> Unlike earlier centralized P2P file-sharing programs which rely upon a single facility for identifying files, the new generation of P2P file sharing programs allow an internet user to access the files located on other computers through the internet. By utilizing the new technology, an internet user can search directly the MP3 file libraries of other users, with no web site being involved because the transferred files are not stored on the computers of the ISP providing the peer-to-peer users with internet access.[135]

In order to pursue their copyright claims against such infringers, copyright holders need to know who they are.[136] The most expeditious method of obtaining this information, and one which minimizes the litigation burden upon ISPs, is to obtain the identities of alleged infringers from ISPs through the use of Section 512 Subpoenas.[137]

> When copyright owners or their representatives learn of a person engaging in infringing activity, they can simply contact the person directly to stop the infringement or else bring a lawsuit to achieve that same result. However, because the alleged infringers . . .

---

holder] must be able to identify the individuals who may be sharing or trading P2P programs. This can be done by obtaining the internet protocol . . . address for a particular screen name, which then can be used to trace the user to the ISP." (citations omitted)); *see also Verizon III*, 351 F.3d at 1232-34 '("Only the ISP . . . can link the IP address used to access a P2P program with the name and address of a person—the ISP's customer—who can then be contacted or, if need be, sued by the RIAA."); Justin D. Fitzdam, *Private Enforcement of the Digital Millennium Copyright Act: Effective Without Government Intervention*, 90 CORNELL L. REV. 1085, 1086 (2005); Andres Sawicki, *Repeat Infringement in the Digital Millennium Copyright Act*, 73 U. CHI L. REV. 1455, 1457 (2006). *See generally* David L. Hayes, Today's Advanced Copyright Issues & Strategies on the Internet, Remarks at the Georgetown University Law Center Continuing Legal Education (Mar. 4, 2004), *available at* 2004 WL 2797059, at 28-29; Mtima, *Copyright Controversies*, *supra* note 27, at 83.

134. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 773 (8th Cir. 2005); *Verizon III*, 351 F.3d at 1232; Alan C. Chen, *Copy Locally, Share Globally: A Survey of P2P Litigation Around the World and the Effect on the Technology Behind Unauthorized File Sharing*, 19 INTELL. PROP. & TECH L.J. 1, 3-4 (2007).

135. *See In re Charter*, 393 F.3d at 773.

136. *Verizon III*, 351 F.3d at 1232.

137. *See* DRATLER, *supra* note 45, § 6.05 ("Without the service provider's assistance, the complaining party may have no way of determining who the real infringer is. That assistance may not be forthcoming without the compulsion of a subpoena, either because the service provider is bound by contract or by law to respect its users' privacy, or because the cumulative financial and administrative burdens of assisting in many such cases motivate the service provider to decline as a matter of policy. Consequently, the complainant must have the compulsion of law in order to force the service provider to divulge the identity of the person responsible for the infringement.").

> identify themselves on the internet only by their screen names, the [copyright holder] has been unable to use ordinary means to identify and contact them.[138]

In most cases, obtaining an alleged infringer's "real world identity" from an ISP is the only way to get this information.[139]

Thus, the ability of copyright holders to obtain Section 512 Subpoenas in connection with Conduit ISPs is vital to the protection of their copyright property rights, and in particular, to maintaining the balance between ISP and copyright holder interests which the Act is designed to achieve. Direct litigation against suspected infringers, as an alternative to litigation against ISPs on grounds of indirect infringement, is one of the key goals the Liability Limitation Act was designed to achieve.[140] Construing sub-section 512(h) to be applicable to Conduit ISPs furthers this statutory objective.

---

138. *In re Subpoena*, 367 F. Supp. 2d at 946.

139. *See In re Charter*, 393 F.3d at 774 ("[B]y using tracking programs, the RIAA ascertained the internet protocol (IP) addresses and user names (e.g., paulina400@KaZaA) of ninety-three Charter subscribers suspected of trading copyrighted music files. The RIAA logged onto P2P networks and observed certain users offering the copyrighted songs for downloading. It confirmed the infringement by downloading files offered by individuals and verifying such as being unauthorized copies of copyrighted sound recordings. The RIAA alleges such subscribers collectively made more than 100,000 copyrighted songs available for illegal copying and downloading. Significantly, with an IP address, the RIAA can identify the ISP providing internet access to an alleged infringing party. Only the ISP, however, in this case Charter . . . can link a particular IP address with an individual's name and physical address."); Elektra Entm't Group, Inc. v. DOES 1-9, No. 04 Civ. 2289, 2004 U.S. Dist. LEXIS 23560, at *4 (S.D.N.Y. 2004) ("An IP address is a 10-digit number that specifically identifies a particular computer using the Internet. Using the IP address, plaintiffs determined that each defendant was using NYU's network facilities to disseminate the plaintiffs' copyrighted works. From the IP address provided by plaintiffs, NYU can match the IP address, date and time with the computer that was using the IP address when plaintiffs observed the alleged infringement. NYU is therefore the only entity that can identify the defendants in this case."); *see also* DRATLER, *supra* note 45, § 6.05[2][a] (describing the complexities of matching an IP address to a "brick and mortar" place and person); Dutcher, *supra* note 98, at 503 (detailing the same problem).

140. *See* H.R. REP. NO. 105-551, pt. 2, at 61 (1998) ("[T]hose who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access."); Raynolds, *supra* note 43, at 347-48 (noting that the purpose of the Act is to forge cooperation between copyright holders and ISPs in addressing Internet infringement and to provide remedies for Internet infringement); Borland, *supra* note 20 (discussing how the *Verizon III* construction of subsection 512(h) has affected the relationship between the copyright content industries and the ISP community).

2. Construing Subsection 512(h) to Mandate ISP Removal of Infringing Material Undermines the Principal Goals of the Liability Limitation Act

When confronted with ambiguous statutory language, a court should strive to construe the statute so as to effectuate its purpose, if it can reasonably do so.[141] Accordingly, in construing such language, courts should look to the relevant legislative history and other pertinent material to ascertain the legislative intent.[142] "If, after . . . review, the Court finds the statutory language in question to be ambiguous, it may look to the legislative history to determine Congressional intent and, if that is not apparent, then it may apply the traditional tools of statutory construction."[143]

Construing sub-section 512(h) so as to exclude Conduit ISPs from its reach undermines the goals of the Liability Limitation Act. The Act was promulgated not only to immunize ISPs from copyright liability in connection with the conduct of their subscribers, but also to preserve the rights of copyright holders against infringing activities on the Internet.[144] Precluding copyright holders from

141. *See* 73 AM. JUR. 2D *Statutes* § 75 (2007) ("[T]he rule that words of a statute are to be taken in their ordinary sense yields when necessary to effectuate the real purpose of the lawgiver, or whenever the case is clearly within the mischief sought to be prevented, and it is proper to depart from the usual and natural, or literal, meaning of words used in a statute, where the application of the literal or commonly accepted meaning would operate to defeat the purpose of the statute."); *see also* Takao Ozawa v. United States, 260 U.S. 178, 194 (1922) ("It is the duty of this Court to give effect to the intent of Congress. Primarily this intent is ascertained by giving the words their natural significance, but if this leads to an unreasonable result plainly at variance with the policy of the legislation as a whole, we must examine the matter further. We may then look to the reason of the enactment and inquire into its antecedent history and give it effect in accordance with its design and purpose, sacrificing, if necessary, the literal meaning in order that the purpose may not fail.").

142. 73 AM. JUR. 2D *Statutes* § 74 (2007) ("The purpose of a statute is to be gathered from the whole act. In determining such purpose, resort may be had, not only to the context, but to the structure and scheme of the act, and in some cases, to its historical background or legislative history."); *see also* Boeve, *supra* note 101, at 129-30 ("Legislative history is important because only Congress is empowered with the authority and the procedural tools necessary to completely serve all those with a stake in the legal implications of a new technology.").

143. *In re Subpoena*, 367 F. Supp. 2d at 951.

144. *See, e.g., Verizon I*, 240 F. Supp. 2d at 33 ("Congress not only sought to limit the liability of service providers under the DMCA, but also intended to assist copyright owners in protecting their copyrights. The legislative history makes clear that in enacting the DMCA, Congress attempted to balance the liability protections for service providers with the need for broad protection of copyrights on the Internet."); *see also* Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004); ALS Scan, Inc., v. Remarq Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001); Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 847 (C.D. Cal. 2006) (finding that the creation of "thumbnails" that are almost the same size as the originals constitutes infringement under the DMCA); Kelly v. Arriba

expeditiously obtaining the identities of suspected infringers from Conduit ISPs contradicts each of these explicit statutory objectives.[145] Accordingly, such a construction of the statute is an

---

Soft Corp., 77 F. Supp. 2d 1116, 1121-22 (C.D. Cal. 1999), *aff'd in part, rev'd in part*, 280 F.3d 934 (9th Cir. 2002), *withdrawn*, 336 F.3d 811 (9th Cir. 2003). *See generally* Boeve, *supra* note 101, at 129 ("When Congress passed the DMCA, its intent was to deal with the "massive piracy" of copyrighted material over the Internet while refraining from smothering the growth of the technology by placing the burden of liability for illegal customer use on ISPs. In doing so, the Act had to accommodate and balance the competing interests of copyright holders and the ISPs. The copyright owners wanted to ensure that their intellectual property would be protected by minimizing the threat that Internet piracy posed. On the other hand, the ISPs wanted limitations on liability for illegal customer use of their Internet services. Congress sought to foster cooperation between ISPs and copyright owners by creating incentives for ISPs to detect and stop infringing activity and by eliminating uncertainty for ISPs regarding exposure to third party liability for contributing to their customers" copyright infringement."); Elkin-Koren, *supra* note 45, at 348 (arguing that the imposition of copyright liability on ISPs undermines the open discourse structure of the Internet); Ludwig, *supra* note 20, at 1, 3 ("Internet Service Providers (ISPs) are an essential component of the internet: they enable users and content providers to connect with one another online. In enacting the Digital Millennium Copyright Act (DMCA), the purpose of which was to strengthen copyright protections in the digital realm, Congress recognized both the important role played by ISPs and the danger of copyright infringement liability for ISPs under existing case law. . . . Congress therefore sought to strike a balance in which service providers and intellectual property rights holders would cooperate in the enforcement of intellectual property rights online against actual repeat infringers and those who traffic in technologies that enable infringers to circumvent the technological self-help measures of intellectual property rights holders." (footnotes omitted)); Mtima, Tasini *and Its Progeny*, *supra* note 26, at 422-26 (explaining that Internet use of copyrighted works currently falls with the copyright holder's exclusive rights and should be regarded by the courts as such until Congress indicates otherwise).

145. *See* Ravn, *supra* note 27, at 785-86, 787 ("Unrestrained, misguided, and inconsistent application of [copyright indirect liability] could have had a disastrous impact upon the future of the Internet. Placing liability for contributory and vicarious infringement onto OSPs would have impacted upon their ability to organize information and increase the cost of their services to users. The threat of liability might have deterred web sites, OSPs, and logical access providers from using hyperlinks. The less often hyperlinks are used and the fewer logical access providers who are willing to take such risks, the more difficult it would become for Internet users to navigate the Web. Ultimately, the Internet may have ceased to be a 'seamless web' of interconnected documents—thereby substantially decreasing its utility. . . . Congress's answer to the possible dangers posed by the courts" inconsistent application of the copyright law to the Internet terrain was to provide certain 'safe harbors'—to condition the provision of exemptions sought by OSPs upon compliance with procedural safeguards designed to protect the interests of copyright owners. In Conference Report 796, Congress explained that Title II 'preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment' while also providing 'greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.'" (footnotes omitted)). The alternative and burdensome course for copyright holders would be to undertake

undesirable resolution of any purported ambiguity therein, and should not be favored over an alternative construction which can both resolve any such ambiguity and also achieve the statute's goals.[146]

Perhaps one reason that the *Verizon III* court did not embrace a more viable interpretation of the purported 512(h) ambiguity is the manner in which the issues were framed by the litigants before the court. For example, in *Verizon III,* the RIAA did not argue that the asserted ambiguity in 512(h) could be resolved in a manner that would implement the purpose of sub-section 512(h).[147] Instead, the

---

'John Doe' suits and obtain the information from ISPs through third-party discovery. *See, e.g.*, Raynolds, *supra* note 43, at 372-73 ("John Doe litigation is unnecessarily burdensome to copyright owners because Congress has devised a process that provides copyright owners with a remedy against infringement in the form of the [Section 512 Subpoena]. John Doe litigation would, among other things, require plaintiffs to pursue third party subpoenas to seek defendant identification. This is burdensome because the time and delay associated with filing complaints and pursuing third-party subpoenas in court would undermine the ability of copyright owners to act quickly to prevent further infringement of their copyrights. That is at odds with the design of Congress through the DMCA, which commands '"expeditious"' issuance of and response to subpoenas under subsection (h).") *But cf.* Kao, *supra* note 11, at 417-18 (discussing the potential impact of Section 512 Subpoenas on ISPs: "[I]n enacting the [DMCA] Congress intended to limit the liability of ISPs, in addition to securing the rights of copyright holders . . . . Therefore, the burden carried by the ISP in enforcing the subpoena provision is a crucial consideration, particularly because the assessment is complicated by another new technology development in addition to P2P software—that is, the use of 'bots,' a software tool used by copyright owners to monitor the Internet and detect unauthorized distribution of copyrighted material . . . . [B]ots' would inundate service providers with thousands of computer-generated subpoenas seeking to identify infringers. . . . All ISPs would be required to answer these subpoena requests or risk liability. Some have considered the staggering number of requests to be an attempt at ISP harassment, and owners of smaller ISPs have complained that they are unable to afford to keep up with the number of requests and are at risk of becoming so overwhelmed that they may actually be driven out of business. It seems unlikely that Congress would have enacted the DMCA to have this end result, when the purpose of 512 was to place limitations on the liability of ISPs, not to burden them further.").

146. *See* Chapman v. Houston Welfare Rights Org., 441 U.S. 600, 608 (1979) ("As in all cases of statutory construction, our task is to interpret the words of these statutes in light of the purposes Congress sought to serve."); *see also* Shapiro v. United States, 335 U.S. 1, 31 (1948) (holding that where a statute is susceptible of either of two opposed interpretations, it must be read in the manner which effectuates rather than frustrates the major purpose of the legislature); United States v. Ryan, 284 U.S. 167, 175 (1931) ("A literal application of statute leading to absurd consequences is to be avoided whenever reasonable application can be given consistent with legislative purpose."). Indeed, the court in *In re Subpoena* acknowledged that construing subsection 512(h) to be applicable to Conduit ISP seems consist with the purpose of the Act, but declined to adopt such construction out of a concern that the court might be rewriting and not merely interpreting the actual words employed in the statute. *See In re Subpoena,* 367 F. Supp. 2d at 954.

147. *Verizon III,* 351 F.3d at 1235.

RIAA focused on the purpose of sub-section 512(c), and essentially argued that Conduit ISPs can "substantially" comply with the "take-down" requirement of sub-section 512(c), because once an infringing subscriber has been identified, the Conduit ISP can disable the subscriber's Internet connection, and in that way "remove" any infringing material from the Internet.[148]

The *Verizon III* court correctly found the RIAA's "substantial compliance" argument unavailing. Disclosing the identity of an alleged infringer and removing infringing material from the Internet are two distinct remedies, and the provision of a 512(c) Notice in connection with a Section 512 Subpoena does not (and need not) result in any "substantial satisfaction" of the 512(c) "take-down" function.[149] What the RIAA should have argued is that nowhere does the Act state that the *only* purpose a 512(c) Notice can ever serve is effectuating the removal of infringing material. Rather, the Act as a whole is concerned with achieving removal of infringing material and/or identifying alleged infringers, as appropriate. While the 512(c) Notice information can aid in implementing a "take-down" in connection with 512(b) through (d), it can also aid in implementing infringer identification in connection with 512(h). Consequently there is no need to argue that the provision of infringer subscriber identities in response to a Section 512 Subpoena "substantially accomplishes" a sub-section 512(c) infringing material "take-down."

The *Verizon III* court also expressed the concern that perhaps Congress had not intended for Section 512 Subpoenas to be used in connection with Conduit ISPs, because Congress could not have anticipated the development of P2P file sharing technology and anonymous mass distribution of copyrighted material.[150] Internet users previously engaged in the mass distribution of copyrighted material by uploading it to centralized locations on the Internet, such as electronic bulletin boards, which would constitute Storage ISPs.[151] The advent of P2P technology, however, has enabled users to

148. *See id.*

149. The reference in 512(h) calls only for notice as *described* in 512(c)(3) and does not require that such notice be *effective* under 512(c), thus the notice accompanying the Section 512 Subpoena need not be capable of identifying or leading to the removal of infringing material, whether directly or indirectly, such as through the disabling of the Internet connection of the infringing end-user. *See* discussion *supra* Part IV.A.1.

150. *Verizon III*, 351 F.3d at 1238 ("[T]he legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works. . . . The Congress had no reason to foresee the application of § 512(h) to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along. Had the Congress been aware of P2P technology, or anticipated its development, § 512(h) might have been drafted more generally.").

151. *See* discussion *supra* Part I.

anonymously distribute material *directly* to other users, and thereby eschew ISP storage of transmitted material.[152]

The subsequent development of a new technological means by which to use copyrighted works is expressly anticipated by the Copyright Act.[153] The Copyright Act makes clear that the mere fact that a specific technology did not exist when the statute was passed or amended does not mean that the technology is automatically beyond the purview of the statute.[154] Rather, courts undertake a substantive approach, to determine whether the new technological use constitutes a methodology substantially similar to that of pre-existing methods of use.[155]

---

152. *See, e.g.*, Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd., 544 U.S. 903 (2005); In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); Hendrickson v. Amazon.Com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003); Chen, *supra* note 134, at 3-4.

153. *See* 17 U.S.C. § 102(a) (2006) ("Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression, now known or later developed . . . ."); *see also* H.R. REP. NO. 94-1476, at 52 (1976) ("As a basic condition of copyright protection, the bill perpetuates the existing requirement that work be fixed in a 'tangible medium of expression,' and adds that this medium may be one 'now known or later developed,' and that the fixation is sufficient if the work 'can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.' This broad language is intended to avoid the artificial and largely unjustifiable distinctions, derived from cases such as *White-Smith Publishing Co. v. Apollo Co.*, 209 U.S. 1 (1908), under which statutory copyrightability in certain cases has been made to depend upon the form or medium in which the work is fixed. Under the bill it makes no difference what the form, manner, or medium of fixation may be—whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device 'now known or later developed.'" (footnote omitted)); *see also* Williams Elecs., Inc. v. Artic Int'l, Inc., 685 F.2d 870, 877 & n.8 (3d Cir. 1982) ("A 'copy' is defined to include a material object in which a work is fixed 'by *any* method now known or later developed, and *from which the work can be perceived*, reproduced, or otherwise communicated, either directly or with the aid of a machine or *device*.' By this broad language, Congress opted for an expansive interpretation of the terms 'fixation' and 'copy' which encompass technological advances such as those represented by the electronic devices in this case . . . . The legislative history of the 1976 Copyright Act supports this interpretation. It emphasizes the expanded scope of the fixation requirement." (citation omitted)).

154. *See, e.g.*, Advance Magazine Publishers, Inc. v. Leach, 466 F. Supp. 2d 628, 637 (D. Md. 2006) ("Plaintiff contends that Defendant violated its exclusive right to reproduce the publications by scanning into electronic form the text, original illustrations, and cover art of its publications. It is well-established that photocopying a copyrighted work without the owner's permission infringes the owner's right of reproduction. Although Defendant used a scanner to create a digital copy of a work, rather than a photocopier to print a physical copy, the methods of copying are equivalent and they are both infringing." (citations omitted)); *see also* Mtima, Tasini *and Its Progeny, supra* note 26, at 449-52 (discussing judicial application of the copyright law to new technological uses of copyrighted works).

155. *See Advance Magazine Publishers*, 466 F.Supp. 2d at 637; *see also* Boosey &

Thus, the fact that P2P technology was not prevalent when the Liability Limitation Act was passed does mean that this method of Internet distribution is beyond the purview of the DMCA.[156] In subsection 512(a), Congress set forth a safe harbor for Conduit ISPs without reference to any specific technological devices that their subscribers might utilize once connected to the Internet, or to the specific kinds of activities such subscribers might engage in.[157] Accordingly, while certainly not inexorable, it is reasonable to conclude that Congress did not intend for the applicability of subsection 512(h) to be dependent upon the specific methodologies deployed by a Conduit ISP's individual subscribers.[158] Thus, whether a subscriber uses her Conduit ISP connection to connect to an electronic bulletin board or to log onto a P2P network, the Conduit ISP's DMCA protections (and obligations) would remain the same. Such a construction of sub-section 512(h) seems more consistent with the application of the Copyright Act as a whole.[159]

Hawkes Music Publishers, Ltd. v. Walt Disney Co., 145 F.3d 481 (2d Cir. 1998); Cohen v. Paramount Pictures Corp., 845 F.2d 851 (9th Cir. 1988); Bartsch v. Metro-Goldwyn-Mayer, Inc., 391 F.2d 150 (2d Cir. 1968). *See generally* Joanne Benoit Nakos, *An Analysis of the Effect of New Technology on the Rights Conveyed by Copyright License Agreements*, 25 CUMB. L. REV. 433 (1995); Sidney A. Rosenzweig, Comment, *Don't Put My Article Online!: Extending Copyright's New-Use Doctrine to the Electronic Publishing Media and Beyond*, 143 U. PA. L. REV. 899, 906 (1995).

156. *See* DRATLER, *supra* note 45, § 6.05[2][b] ("[W]hile the court of appeals made much of the fact that peer-to-peer technology was unknown to Congress in 1998, when Section 512(h) became law, it neglected substantial evidence that Congress did not intend to leave such a yawning loophole in subsection (h). In analyzing congressional intent, the court of appeals cited testimony in congressional hearings in which specific technologies of transmission were discussed. It failed, however, to note the Senate and House Reports, both of which state that subsection (h)'s subpoena power was intended to allow a copyright owner to 'obtain an order for identification of alleged infringers who are users of a service provider's system or network.' While far from conclusive, these excerpts suggest that what Congress intended was a broad and general subpoena power that does not depend on the particular technology of transmission used for infringement."); Raynolds, *supra* note 43, at 375 ("The DMCA 'sought to provide assistance to copyright owners in light of the technological developments surrounding the Internet.' The idea was to create a flexible law that could be meaningful in light of technological improvements—not to develop a limited statute that would become inapplicable as technology improves.").

157. *See* 17 U.S.C. § 512(a)-(d) (2006).

158. *See* DRATLER, *supra* note 45, § 6.05[2][b] (applying a similar argument to end-user infringement undertaken by attaching copyrighted material to private emails).

159. Moreover, in her dissent Judge Murphy argued that Congress *did* intend that the specific problem of P2P file-sharing be addressed by Section 512 Subpoenas. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 779 (8th Cir. 2005) (Murphy, J., dissenting). She explained that:

> The increasing use of peer to peer file sharing programs makes the DMCA subpoena power very significant. Such programs were already being developed at the time of the congressional hearings preceding the passage of

In contrast to the reasoning of the majority in *Verizon III*, Judge Murphy employed such a social-balancing lens in examining the Liability Limitation Act in her dissenting opinion in *In re Charter*.[160] In Judge Murphy's view, the majority in *In re Charter* (and the court in *Verizon III*) "focuses too narrowly in its reading of the DMCA, overlooks certain plain language used by Congress, and fails to give effect to the statute as a whole."[161] Considering the overall purpose of the Liability Limitation Act, Judge Murphy concluded that the majority had adopted an unrealistic construction of the statute:

> In enacting the DMCA Congress sought to protect both the interests of copyright holders and of internet service providers concerned about their own liability for infringement by their customers. The legislative solution in response to these concerns significantly limited the liability of ISPs for infringement by their customers and provided copyright holders more direct means to attack digital piracy. The subpoena provision in § 512(h) is one of these means, and this provision is of special value to a copyright owner seeking to stop infringement through conduit service providers. That is because a conduit ISP does not store materials for downloading and thus cannot directly remove or disable access to any infringing material. By using the § 512(h) subpoena power to learn the identity of conduit service subscribers who infringe, copyright holders are able to take steps to protect their interests, seek compensation for their misappropriated property, and stop infringement.[162]

Pursuing this rationale, Judge Murphy offered alternative constructions of the contested sections of the Act, which would preserve the overall purpose of the Act.[163] Both the constructions proffered by Judge Murphy and the arguments asserted herein provide viable interpretations of the Act consistent with Congress's intent—interpretations that should be adopted over the *Verizon III* rationale, which undermines the statutory objectives.

C. Applying Section 512 Subpoenas to Conduit ISPs Furthers Copyright Social Policy

In addition to achieving the specific goals of the Liability

---

the DMCA. Congress recognized the need to address infringement through conduit service providers in the DMCA, and its opening section applies to networks which transmit infringing materials at the direction of their users.

Id. (citation omitted).

160. *See id.* at 778-86.

161. *Id.* at 778.

162. *Id.*

163. For example, Judge Murphy suggested that one reason for including the 512(c) Notice is to aid in determining specifically what material is the subject of the copyright holder's infringement claims. *See id.* at 780-83.

Limitation Act, extending Section 512 Subpoenas to Conduit ISPs is also consistent with copyright social policy as a whole. In accordance with Article I, Section 8 of the Constitution, Congress has relegated certain uses of copyrighted works exclusively to copyright holders, including the rights to reproduce or distribute such works.[164] Congress has determined that this particular allocation best promotes the advancement of the arts and sciences in American society.[165]

---

164. *See, e.g.*, Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 546-47 (1985) ("Section 106 of the Copyright Act confers a bundle of exclusive rights to the owner of the copyright. Under the Copyright Act, these rights—to publish, copy, and distribute the author's work—vest in the author of an original work from the time of its creation. In practice, the author commonly sells his rights to publishers who offer royalties in exchange for their services in producing and marketing the author's work." (footnotes and citations omitted)); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1366-67 (N.D. Cal. 1995) ("To establish a claim of copyright infringement, a plaintiff must demonstrate (1) ownership of a valid copyright and (2) 'copying' of protectable expression by the defendant. Infringement occurs when a defendant violates one of the exclusive rights of the copyright holder. These rights include the right to reproduce the copyrighted work, the right to prepare derivative works, the right to distribute copies to the public, and the right to publicly display the work." (citations omitted)); Mtima, Tasini *and Its Progeny, supra* note 26, at 415-17 ("A claim of copyright infringement in the electronic media/digital re-publication context involves the same sequential analysis as in assessing infringement claims raised in connection with traditional media. First, the court must determine that the plaintiff has demonstrated ownership of a valid copyright. Second, the plaintiff must adduce evidence that the defendant has engaged in one or more of the exclusive rights in connection with original constituent elements of the copyrighted work. Where there is no dispute regarding the validity of the plaintiff's copyright, analysis of the infringement claim begins with a determination of whether the unauthorized electronic publication involves one or more of the exclusive rights, and if so, which ones. Once it has been established that the unauthorized electronic activity involves one or more of the exclusive rights, the resolution of the infringement claim will turn on the nature of the defense raised in support of the unauthorized use. Unless the infringement defendant asserts some claim of license, he or she must rely instead upon one of the copyright defenses that permit engagement in the exclusive rights without the copyright holder's consent."). *But cf.* Steven D. Jamar, *Copyright and the Public Interest from the Perspective of* Brown v. Board of Education, 48 HOW. L.J. 629, 639 (2005) ("The Copyright Act creates a number of rights that attach to original works of authorship fixed in a tangible medium of expression. But, many of those rights are subject to limitations and exceptions in the Copyright Act itself for reasons of public policy. These limitations serve to balance some of the competing interests among creators, owners, marketers, users, consumers, and others. In some instances, the limitations affect the public interest in developing information and advancing the arts and sciences. That is, Congress decided that the rights should be limited and various uses that would otherwise infringe should be permitted. These limitations do not result in the works being put in the public domain, but they do make lawful certain uses of the works that would otherwise be infringing.").

165. *See Harper & Row*, 471 U.S. at 558 ("The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance public

Notwithstanding consistent confirmation from the courts that the copyright holder's exclusive rights of reproduction and distribution encompass Internet dissemination, the problem of illegal file sharing and other forms of Internet copyright infringement remains a continuing threat to the copyright regime[166]:

> Individuals with a personal computer and access to the internet

---

welfare through the talents of authors and inventors in Science and useful Arts." (quoting Mazer v. Stein, 347 U.S. 201, 219 (1954) (internal quotation marks omitted))); Sony Corp. of Am. v. Universal Studios, Inc., 464 U.S. 417, 429 (1984); Paul Goldstein, COPYRIGHT 1.14 (2d ed. 2002); Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1107 (1990) ("The Supreme Court has often and consistently summarized the objectives of copyright law. The copyright is not an inevitable, divine, or natural right that confers on authors the absolute ownership of their creations. It is designed rather to stimulate activity and progress in the arts for the intellectual enrichment of the public."); Mtima, Tasini *and its Progeny*, *supra* note 26, at 396-97 ("Pursuant to article I, Congress has the power 'to 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 . . . .' In accordance with this constitutional mandate, both Congress and the courts have determined that the 'overarching object of copyright law in the United States is to encourage the widest possible production and dissemination of literary and artistic works.' Through widespread production and dissemination, the greatest amount of creative works are likely to reach the largest audience, who will not only benefit from exposure to these works, but who will in turn build upon the ideas advanced therein and produce additional works. . . . In order to achieve such widespread dissemination of creative works, however, there must first be an abundant supply of creative works to disseminate. Consequently, creative artists must have proper incentive to produce these works. . . . Congress may provide such incentive by granting authors the 'exclusive right' to their works. By securing to authors property rights in connection with their works, the copyright law provides a means by which authors might profit financially from their efforts and thereby provides them with the necessary inducement to undertake and continue their creative labors." (first alternation in original) (footnotes omitted)).

166. *See, e.g.*, Chen, *supra* note 134, at 1; Edwards, *supra* note 132, at 835-41 (recounting the history of illegal file-sharing and the Napster Litigation); Veasman, *supra* note 47, at 314-15, 317-18 ("Today's World Wide Web ('Web 2.0') is a new and improved version from the Web of the past ('Web 1.0'). Web 2.0 is the term commonly used to refer to "'technology that encourages sharing, user input and community.'" Specifically, it is a second generation of Web-based services, including blogs, social networking sites, RSS feeds, podcasts, Web APIs, and mashups. . . . Web 2.0 makes user-generated content and interaction possible because, rather than using the PC as its platform as Web 1.0 does, Web 2.0 uses the Internet as its platform. Typical user interaction in the world of Web 2.0 includes tagging content or contributing user content through podcasts, social networking, or blogging. . . . As the American population continues to discover Web 2.0, more and more people use its activities and applications regularly. . . . Possible copyright infringement actions that occur online include: consumer uploading files; knowingly and unknowingly offering copyrighted material for display by the way of web browsing; performing a copyrighted work by way of streaming audio or video or downloading; and sending email. While the individual who posts the infringing material is the obvious target for direct infringement, the website may also face liability.").

> began to offer digital copies of recordings for download by other users, an activity known as file sharing, in the late 1990's using a program called Napster. Although recording companies and music publishers successfully obtained an injunction against Napster's facilitating the sharing of files containing copyrighted recordings millions of people in the United States and around the world continue to share digital .mp3 files of copyrighted recordings using P2P computer programs such as KaZaA, Morpheus, Grokster, and eDonkey. . . . To date, owners of copyrights have not been able to stop the use of these decentralized programs.[167]

Indeed, Internet technology advances continue to outpace the ability of the courts to address them individually. It seems that as soon as the courts outlaw a specific kind of Internet infringement conduct, new methods for the unauthorized "e-distribution" of copyrighted material become available, and the legal chase begins anew.[168] The public becomes familiar with a new method for

---

167. *Verizon III*, 351 F.3d at 1231-32 (citing A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1099 (9th Cir. 2002) (citations omitted)); *see also In re Charter*, 393 F.3d at 773 ("Advances in technology . . . including the use of MP3 format (a compressed digital format) facilitated [Internet] piracy, and by 1998 approximately three million sound recordings were believed to be downloaded from the internet daily. In 1999, such activity reached new heights with the emergence of so-called peer-to-peer (P2P) systems. Like BBS sites, P2P systems allow users to disseminate files stored on their computers to other internet users."); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Advance Magazine Publishers, Inc. v. Leach, 466 F. Supp. 2d 628 (D. Md. 2006). *See generally* John Borland, *File Swapping Shifts Up a Gear*, CNET NEWS, May 27, 2003, http://news.cnet.com/2100-1026-1009742.html.

168. *See, e.g.*, Constance S. Hawke, *Piracy Tools and Protocols: Information on University Networks*, 209 ED. LAW REP. 17, 20-21 (2006) ("At the same time that legislation has changed the legal landscape of copyright infringement, the technology continues to evolve . . . . In 1998-the year the DMCA was enacted-approximately three million sound recordings were downloaded from the internet on a daily basis. In 1999, the technology for peer-to-peer (P2P) systems emerged . . . . P2P technology allows internet users to search directly the file libraries on other users' personal computers . . . . Estimates are that more than 2.6 billion music files are downloaded monthly. In light of the escalating infringement of copyrighted music, the owners and creators of copyrighted music initiated lawsuits against the operators of P2P file sharing services."). *See generally* Jamar, *supra* note 164, at 630-32 ("In recent years, significant academic attention has been directed toward defining the proper limits of legal protection for intellectual property. This attention is due to several converging trends. [One] trend . . . is the ever-expanding opportunity to copy and distribute copies of protected works through new, improved, and easy-to-use technologies. Photocopiers, computers, networks, the Internet, and various software applications make sharing files easy and inexpensive. The related facts of the constantly increasing power of computers and software, and the constantly lower prices for affected technologies make copying increasingly easy. The music industry has claimed to be plagued by the ease of copying and distribution, but it has finally stopped fighting the Internet and is actively seeking ways to make money distributing music on it. . . . [Another] trend is the increasing amount of information and works being made readily available online—some of which is in the public domain, some of which seems to be (because it is so

unauthorized Internet distribution and engagement therein soon becomes widespread; copyright holders are then moved to seek redress in the courts, and the new method of unauthorized Internet use is added to the express list of activities that constitute copyright infringement.[169]

Since the passage of the DMCA and the Liability Limitation Act, copyright holders have increased their efforts to proceed directly against individual Internet infringers,[170] limiting the involvement of

---

widely available) but is not, and some of which is clearly not in the public domain, but is available as if it were. This phenomenon contributes to the reconfiguration of the de facto contours of the public domain." (citations omitted)).

169. *See, e.g.*, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004); *In re* Aimster Copyright Litig., 334 F.3d 643, 643 (7th Cir. 2003); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001); Sony Pictures Home Entm't Inc. v. Lott, 471 F. Supp. 2d 716, 721 (N.D. Tex. 2007); Hendrickson v. Amazon, Inc., 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003); The Rodgers & Hammerstein Org. v. UMG Recordings, Inc., No. 00 Civ. 9322, 2001 WL 1135811, at *9 (S.D.N.Y. 2001). *But see* Jamar, *supra* note 164, at 650-51 ("We live in a quicksilver technological environment with courts ill-suited to fix the flow of internet innovation. The introduction of new technology is always disruptive to old markets, and particularly to those copyright owners whose works are sold through well-established distribution mechanisms. Yet, history has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine, or an MP3 player. Thus, it is prudent for courts to exercise caution before restructuring liability theories for the purpose of addressing specific market abuses, despite their apparent present magnitude." (citations omitted)); Stacy F. McDonald, Note, *Copyright for Sale: How the Commodification of Intellectual Property Distorts the Social Bargain Implicit in the Copyright Clause*, 50 HOW. L.J. 541, 543-44 (2007) ("After recent years of litigation and legislation, fueled by rapid technological change, instead of a social bargain 'we now survey a battlefield that pits private interests against the public good . . . .' One cause of these copyright battles is a commodification mentality, a subtle, yet acute, shift in the conceptualization of copyright law that has upset the balance. When viewed through this commodification lens, a copyrighted work looks like an 'undifferentiated product,' such as wheat or oil, whose market value stems solely from the owner's right to sell it. A copyrighted work becomes valued for its profitability, rather than its contribution to education, public discourse, or intellectual enlightenment. . . . [T]he commodification of intellectual property distorts the copyright balance by valuing a copyrighted work for its market potential over, above, and to the exclusion of its non-economic values. Rather simplistically, the content industry believes that the public is benefited solely because the products are on the market, ready for mass consumption. This commodification mentality excises from the equation the social bargain inherent in the Copyright Clause, as well as what the Framers considered to be the goals of the copyright system.").

170. *See* Mark Stodghill, *Duluth Jury Orders Brainerd Women to Pay $222,000 for Distributing Music Files*, DULUTH NEWS TRIBUNE, Oct. 5, 2007 ("A jury of 12 . . . decid[ed that Jammie Thomas was] liable for $222,000 in damages for willfully committing copyright infringement by distributing 24 songs on the KaZaA peer-to-peer file sharing network. . . . The record companies alleged that SafeNet, their anti-piracy contractor, found a KaZaA user called 'tereastarr' offering 1,702 songs for others to download on Feb. 21, 2005. SafeNet downloaded tracks whose copyrights belonged to

ISPs primarily to removing infringing material and/or providing the identities of suspected infringers.[171] Until recently there was little question that the Section 512 Subpoena constitutes an indispensable tool in any strategy to pursue Internet infringers, and thereby extricate ISPs from copyright holder/ISP subscriber skirmishes.[172]

> The RIAA now has begun to direct its anti-infringement efforts against individual users of P2P file sharing programs. In order to pursue apparent infringers the RIAA needs to be able to identify the individuals who are sharing and trading files using P2P programs. The RIAA can readily obtain the screen name of an individual user, and using the Internet Protocol (IP) address associated with that screen name, can trace the user to his ISP. Only the ISP, however, can link the IP address used to access a P2P program with the name and address of a person—the ISP's customer—who can then be contacted or, if need be, sued by the RIAA.[173]

Given the particular problem that Congress sought to address in passing the Liability Limitation Act, and the fact that the problem worsens daily, an interpretation that finds Section 512 Subpoenas to be applicable to Conduit ISPs is a socially responsible construction of the statute. "[Congress's] balancing effort resulted in a statute that creates 'strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital network environment.'"[174]

---

the record companies and linked them to Thomas's Internet address with Charter Communications."); *see also* Chen, *supra* note 134, at 1, 3.

171. *See, e.g.*, *Verizon III*, 351 F.3d at 1234; Warner Bros. Records, Inc. v. Souther, No. 1:05CV279, 2006 WL 1549689, at *6-8 (W.D.N.C. June 1, 2006); *Hendrickson*, 298 F. Supp. 2d at 916; Eric J. Sinrod, *RIAA Music Lawsuits Chill Online Downloading*, USA TODAY, Jan. 14, 2004, http://www.usatoday.com/tech/columnist/ericjsinrod/2004-01-15-sinrodx.htm.

172. *See, e.g.*, *Verizon III*, 351 F.3d at 1232.

173. *Id.*

174. *See In re* Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 779 (8th Cir. 2005) (Murphy, J., dissenting) ("Copyright laws were foreseen by the framers of the Constitution as '"the engine of free expression."' . . . Piracy substantially undermines this incentive. Annual losses to copyright owners even before the expansive growth in peer to peer file sharing were estimated to be $11 to $20 billion. Since copyright holders are effectively unable to recover from the designers of file trading software . . . or from internet service providers . . . action against identified infringers offers the only practical means to protect the interests of copyright holders." (quoting Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985)) (citations omitted)); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 948 (M.D.N.C. 2005) (quoting H.R. REP. NO. 105-551, pt. 2, at 49 (1998)); *see also* Rossi v. Motion Picture Ass'n of Am., Inc., 391 F.3d 1000, 1003 (9th Cir. 2004) ("Title II of the DMCA contains a number of measures designed to enlist the cooperation of Internet and other online service providers to combat ongoing copyright infringement."); Yen, *supra* note 17, at 1887-88 ("To the extent that society wants to

In contrast, the construction of sub-section 512(h) adopted in *Verizon III* and its progeny does little to effectuate Congress's copyright balancing goals. Indeed, it not only fails to implement the legislative intent, it directly undermines it. Pursuant to sub-sections 512 (a) and (j), even if Section 512 Subpoenas are unavailable against Conduit ISPs, copyright holders remain free to obtain the identities of alleged infringers from such ISPs through other means, including traditional discovery in the course of civil litigation.[175] Thus, the *Verizon III* construction of sub-section 512(h) will actually lead to a return to "indirect" litigation against Conduit ISPs, prolonging the involvement of ISPs in individual litigation disputes in which they have no immediate stake.[176]

---

protect the interests of content providers and ISPs, the DMCA's safe harbors make sense. Content providers now have a quick and inexpensive way to remove material that they believe is infringing. This arguably serves society's interest by making copyright rights more valuable and productive. Those who commit infringement on the Internet will cut into the content provider's profits for a shorter duration, thereby preserving copyright's incentive for the creation of new works. ISPs also will flourish because they need not fear liability for the acts of their subscribers. This in turn might make Internet access less expensive to future subscribers.").

175. *See, e.g., In re Charter,* 393 F.3d at 775 n.3 ("[O]rganizations such as the RIAA can also employ alternative avenues to seek this information, such as 'John Doe' lawsuits. In such lawsuits, many of which are now pending in district courts across the country, organizations such as the RIAA can file a John Doe suit, along with a motion for third-party discovery of the identity of the otherwise anonymous 'John Doe' defendant."); CALIFORNIA SUBPOENA HANDBOOK § 6:5 (2006) ("Despite the holding in Verizon II, copyright owners still have a remedy for enforcing their rights against P2P users. Copyright owners can file 'John Doe' lawsuits against P2P infringers and obtain Doe Subpoenas under Rule 45 of the Federal Rules of Civil Procedure."). At the same time, subsection 512(l) indicates that if an ISP fails to qualify for safe harbor immunity, it may still raise the traditional defenses to copyright liability. Thus, a finding that it would be inequitable to permit an ISP to delay disclosure of infringer identities while invoking safe harbor immunity would not render the ISP liable for infringement, but rather, would put the question of liability in issue. While this would seem an even-handed result, it would also mark a return to the pre-DMCA days of copyright holder/ISP litigation- the very situation the Liability Limitation Act was passed to ameliorate. Obviously such a course would increase the burdens upon copyright holder and ISP alike.

176. Indeed, holding Section 512 Subpoenas inapplicable to Conduit ISPs does not lessen the burden for many of the ISPs embroiled in these disputes. *See* Hawke, *supra* note 168, at 23-24 ("If, in fact, the university [ISP] does not "'store'" the infringing material—and therefore cannot remove or disable it—it is possible that [under the *Verizon III* analysis] a court would quash a subpoena requiring the university to produce identifying information. An analysis would first need to be done to determine what category of services is provided. Then an institution would have to choose to incur the time and expense of fighting such a subpoena."); Ed Treleven, *Music Industry Wins UW IDs in File Sharing Case,* WISC. ST. J., Apr. 26, 2007 (discussing district court decision directing the University of Wisconsin to disclose identities of students engaged in unauthorized music file sharing). Moreover, embroiling ISPs in Internet copyright infringement suits could actually work to the detriment of end-user

In addition, Conduit ISPs that embrace the *Verizon III* reasoning could potentially threaten their eligibility for safe harbor immunity under the Act. Arguably, a Conduit ISP who is aware of the identity of a repeat infringer but refuses to disclose expeditiously that information ceases to be an "innocent bystander." Copyright holders might cogently argue that such conduct constitutes a forfeiture of the Act's protections, at least to the extent that any deliberate delay in the disclosure of an infringer's identity exacerbates the harm to the copyright holder.

> The compromise, as enacted in the DMCA, both preserves copyright enforcement on the internet and provides "immunity to service providers from copyright infringement liability for "passive," "automatic" actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider." This immunity, however, is not presumptive, but granted only to "innocent" service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three

---

First Amendment interests, in that ISPs might find it more expedient to disconnect suspected infringers, rather than risk being dragged in to expensive discovery and litigation. Thus, some legitimate end-users would be unnecessarily censored, whereas an inquiry into their transmissions would have revealed an absence of illegal conduct. *See, e.g.*, Elkin-Koren, *supra* note 45, at 68-70 (arguing that the imposition of copyright liability on ISPs undermines the open discourse structure of the Internet); Kreimer, *supra* note 20, at 27-28 ("The strategy of recruiting proxy censors by targeting the weakest link in the chain of communication [such as ISPs] has obvious advantages for regulators. It provides a mechanism for the exercise of authority over otherwise ungovernable conduct. Moreover, it does so at a discount: the cost of monitoring and sanctioning disfavored communications is largely externalized onto the intermediaries who are the subjects of direct regulation. But these advantages come with substantial costs to the system of free expression . . . . An ISP or search engine may mistake a family photo album for child pornography, an AIDS prevention site for obscenity, a political commentary for a 'true threat,' or a parody for a copyright violation . . . . [T]he dominant incentive of intermediaries is to protect themselves from sanctions, rather than to protect the target from censorship . . . . [C]ensorship by proxy is an unavoidably blunt instrument . . . if it is costly to distinguish protected from unprotected speech, the proxy censor is likely to abandon the effort to avoid errors and adopt a conscious policy of prophylactic self-censorship that blocks any content that could precipitate the threat of sanctions." (footnote omitted)); Malla Pollack, *The* Right *to Know? Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment*, 17 CARDOZO ARTS & ENT. L.J. 47, 109 (1999) ("To negate their own possible liability, OSPs [online service providers] and ISPs are required to take down content when notified by the allegedly aggrieved right holder. No court is involved. No process is provided to the censored speaker before this restraint on his or her speech."); Yen, *supra* note 17, at 1836-37 ("Moreover, the extension of ISP liability [for subscriber infringement] would give ISPs powerful incentives to protect their economic interests by removing subscribers" material from the Internet, even when a good case for copyright infringement does not exist. Such indiscriminate censorship conflicts with First Amendment principles and is too high a price to pay for the protection of copyright rights.").

> prongs of 17 U.S.C. §§ 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter, "preserving the strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[177]

Once a Conduit ISP becomes aware of a subscriber's infringement activities it may well have an affirmative duty to take action.[178] Failing to disclose immediately a suspected infringer's identity, particularly if the ISP also chooses to maintain the subscriber's Internet connection, could raise legitimate questions regarding the equity of the ISP's safe harbor immunity.[179] In light of

---

177. *In re Subpoena*, 367 F. Supp. 2d at 947-48 (quoting H.R. CONF. REP. NO. 105-796, at 72 (1998)) (citations omitted); *see also* ALS Scan, Inc. v. Remarq Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001). Although the quotation concerns Storage ISPs and the duty to remove infringing material, given the purpose of the Act, the same rational might be applied to Conduit ISPs who knowingly abet end-user infringers. *See* Jonathan Band & Matthew Schruers, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L.J. 295, 306-08 (2002) (discussing the knowledge requirements necessary to sustain indirect liability under traditional copyright principals and under the DMCA).

178. *See, e.g.*, Perfect 10, Inc., v. CCBill, LLC, 488 F.3d 1102, 1114 (9th Cir. 2007) (discussing a Storage ISP's 512(i) anti-infringement policy obligations and noting that "a service provider may lose immunity if it fails to take action . . . when it is 'aware of facts or circumstances from which infringing activity is apparent.'" (citing 17 U.S.C. § 512(c)(1)(A)(ii) (2006)); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1101, 1104 (W.D. Wash. 2004). ("The DMCA's balancing efforts reflect an understanding that 'there are different degrees of online copyright infringement, from the inadvertent to the noncommercial, to the willful and commercial. . . . Even with proper enforcement procedures, a copyright holder may still demonstrate that the service provider has not satisfied [the Act] if there are specific instances demonstrating that the service provider tolerates repeat copyright infringement by its users." (citations and internal quotation marks omitted)); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) ("Whether a defendant makes a direct copy [of an Internet transmission] that constitutes infringement cannot depend on whether it received a warning to delete the message . . . . This distinction may be relevant to contributory infringement, however, where knowledge is an element." (citation omitted)); *see also* Ginsburg, *supra* note 47, at 596-98 (arguing that ISP immunity is dependent upon a lack of knowledge of subscriber misconduct); Ludwig, *supra* note 20, at 3 ("Congress structured [the ISP] safe harbors such that a service provider that knowingly contributes to a customer's infringement is liable whereas one that is unaware is exempt . . . . Congress did not intend to change the existing rules of copyright law, but rather sought to offer the safe harbor liability limitations as an incentive for online service providers to cooperate with rights holders to protect intellectual property rights in the digital realm." (footnotes omitted)).

179. *In re Charter*, 393 F.3d at 782 (Murphy, J., dissenting) ("The intent of Congress

these considerations, interpreting sub-section 512(h) to encompass Conduit ISPs is consonant with copyright social policy as a whole.

V. BALANCING COPYRIGHT PROTECTION AND INTERNET SUBSCRIBER PRIVACY TO PROMOTE SOCIALLY RESPONSIBLE INTERNET CONDUCT

Construing the Liability Limitation Act to include Conduit ISPs within the purview of Section 512 Subpoenas is more than a question of statutory construction, or even discerning Congressional intent: it is also a modern problem of individual accountability and social responsibility. Notwithstanding a growing body of legislative, educational, and litigation initiatives designed to promote responsible Internet behavior, many Internet users continue to flagrantly violate the personal and property rights of others, engaging in offensive, shocking, and often illegal conduct, most of which would hardly be tolerated in the "brick-and-mortar" world.[180]

---

in enacting the DMCA was to address 'massive piracy'" of copyrighted works over digital networks without hampering technological development of the internet by the threat of third party liability for service providers. ISPs were only shielded from monetary and injunctive liability in exchange for their assistance in identifying subscribers who engage in acts of piracy over their networks and in removing or disabling access of infringers to protected works when technically possible."); *see also* S. REP. NO. 105-190, at 19-20 (1998) ("As provided in subsection (k), Section 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify. Rather, the limitations of liability apply if the provider is found to be liable under existing principles of law. . . . The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement . . . . These subsections also limit injunctive relief against qualifying service providers to the extent specified in subsection [(j)]. . . . To qualify for these protections, service providers must meet the conditions set forth in subsection [(i)] . . . .").

While it may seem harsh to revoke a Conduit ISP's immunity for failing to comply with a Section 512 Subpoena, said ISP's implicit statutory obligations would seem to support such a result. Whereas the Liability Limitation Act expressly delineates the moment at which a Storage ISP risks loss of its safe harbor immunity (upon failure to "expeditiously respond" to a proper 512(c)(3) Notice) the statute does not so specify the circumstances under which a Conduit ISP's knowledge of an end-user's infringement activities destroys the ISP's presumptive state of innocence. Although the Act clearly limits the relief to be obtained against an "innocent" Conduit ISP that is otherwise in compliance with subsection 512(a), it is not axiomatic that the same limitation should apply to a *culpable*, albeit 512(a) compliant, Conduit ISP.

180. In addition to rampant violations of intellectual property rights, the Internet community is continuously besieged by a virtual cornucopia of tortuous conduct. *See, e.g.*, Kreimer, *supra* note 20, at 13-14 ("When communication utilizes the Internet, government finds it more difficult to sanction either speaker or listener. Speakers can hide their identities, impeding direct coercion; they can extend the reach of their communications into foreign jurisdictions that may face legal or practical impediments to exerting control. Even where speakers are theoretically subject to sanctions, the exponential increase in the number of speakers with potential access to broad audiences multiplies the challenge for censors seeking to suppress a message. On the

And as one might expect, much of this inappropriate and illegal activity is facilitated by the fact that Internet dissemination can be undertaken with almost complete anonymity.[181]

As some commentators have rightly observed, it is high time that the intellectual property law be construed within the context of social

---

listeners' side, an expanding universe of seekers of forbidden content can obtain access to material in private without leaving their homes, bypassing both formal and informal obstacles, and can pursue alternative pathways when a particular route is blocked. The mantra is that 'the Internet interprets censorship as damage, and routes around it.'" (footnotes omitted)); Cara J. Ottenweller, *Cyberbullying: The Interactive Playground Cries For A Clarification of the Communications Decency Act*, 41 VAL. U. L. REV. 1285 (2007) (discussing the problem of "cyberbullying," wherein teens create websites to humiliate and embarrass unpopular and other vulnerable schoolmates); Sharon K. Sandeen, *In For A Calf Is Not Always In For A Cow: An Analysis of the Constitutional Right of Anonymity As Applied to E-Commerce*, 29 HASTINGS CONST. L.Q. 527, 543 (2002) ("Balanced against the asserted benefits of anonymity on the Internet are society's interest in preventing fraud and other wrongful behavior. The concern is that anonymity enables fraud and eliminates or substantially reduces the amount of information about one's actions and reputation that is available or traceable. . . . 'This often encourages outrageous behavior without any opportunity for recourse to the law for redress of grievances.'"); David L. Hudson, Jr., *Taming the Gossipmongers*, A.B.A. J., July 2008, at 19 (discussing the efforts of various state authorities to address the problem of "gossip web sites" and the posting of false and defamatory statements); Todd Hollis, *End Web of Deception*, N.Y. DAILY NEWS, May 7, 2007, at 29 (discussing the devastating impact of false and defamatory statements published on the Internet by an anonymous party). *But cf.* Hardy, *supra* note 40, at 1049-50 (discounting the impact of anonymous Internet defamation: "[I]njured plaintiffs . . . can ignore the defamatory remarks or rebut them, and they can count on others to sharply discount the defamatory remarks. . . . The very power of anonymity, in short, is the plaintiff's own protection, for anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make. . . . Coupled with the access to the means of effective response that cyberspace provides to plaintiffs, this devalued quality of anonymous defamation argues that plaintiffs can unilaterally care for themselves. An adequate first response to the issue of anonymous defamatory messages is therefore for the legal system to do nothing, trusting instead to individuals' self-help in the form of the plaintiffs defending themselves through the same cyberspace medium by which they were defamed, and to the general devaluation and lowered importance of defamatory messages that are from anonymous sources."). One problem with this approach, however, is that it could lead to the complete devaluation of the Internet as a valid information resource; once it becomes generally accepted that much of what is communicated on the Internet is unsubstantiated or unreliable, the stigma will likely spread to many valid postings as well.

181. Hardy, *supra* note 40, at 1005; *see* Doe v. Individuals, 561 F. Supp. 2d 249, 251-52 (D. Conn. 2008) (finding anonymous posting of rape threats and other malicious statements about female law students on a law school admissions web site); United States v. Drew, No. CR-08-0582-GW (C.D. Cal. 2008) (creating a fictitious juvenile identity, an adult parent establishes a MySpace account and publicly ridicules a neighborhood teenager, culminating in the teen's suicide). On November 26, 2008, a federal jury returned a criminal verdict against Ms. Drew for computer fraud, who now faces up to three years in prison and $300,000 in fines. *See* Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES, Nov. 26, 2008, at A25.

justice.[182] But justice mandates a balanced scale, and those who seek equity should do equity. Just as it is disingenuous for copyright conglomerates to cry foul at flourishing Internet piracy, while at the same time maintaining exploitative business practices,[183] it is morally vacuous for private individuals to invoke free speech, privacy, and other civil liberties to cloak illegal and other improper acts.[184] The Internet provides revolutionary educational and cultural benefits, but these boons need not be obtained at the expense of equally important social mores and ideals.

The simple truth of the matter is that the theft of intellectual property under cover of "cyber-pseudonyms" is not only a problem for intellectual property owners, it is iniquitous conduct that distorts the public's perception of appropriate Internet behavior.[185] This and

---

182. *See, e.g.*, Christine Haight Farley, *Protecting Folklore of Indigenous Peoples: Is Intellectual Property the Answer?*, 30 CONN. L. REV. 1, 2-4 (1997); K. J. Greene, *"Copynorms," Black Cultural Production, and the Debate Over African-American Reparations*, 25 CARDOZO ARTS & ENT. L.J. 1179, 1180 (2008); Jamar, *supra* note 164, at 629; Mtima, Introduction, *supra* note 17, at 571; Simone A. Rose, *On Purple Pills, Stem Cells, and Other Market Failures: A Case for a Limited Compulsory Licensing Scheme for Patent Property*, 48 HOW. L.J. 579, 581-83 (2005); McDonald, *supra* note 169, at 574.

183. *See* Greene, *supra* note 182, at 1217 ("The legal regimes of IP and contract, situated in a matrix hostile to both Black cultural production and to Black economic autonomy, failed to protect the interests of Black creative artists on a grand scale (notwithstanding that certain individual artists accrued benefit from the system). If the music industry is serious in its rhetoric about 'theft' of IP, it should atone for the theft it itself has facilitated. The entertainment industry is arguably the prime beneficiary of special interest intellectual property legislation that seeks compensation for even trivial uses of intellectual property.").

184. *See* Sunny Hostin, *Online Campus Gossips Won't Show Their Faces*, CNN.COM, Apr. 11, 2008, http://www.cnn.com/2008/CRIME/03/17/sunny.juicy/index.html ("It [JuicyCampus.com] was founded by a Duke alum, a former frat house president who has gone to lengths to keep his identity secret. We tried to reach him for comment. He didn't return our calls or e-mails."); Connie Llanos, *Concerns Raised About Campus Gossip Online After Silliness Turns to Harassment*, L.A. DAILY NEWS, Mar. 28, 2008, at A1 (discussing anonymous college gossip site JuicyCampus.com and California State Assemblyman Alberto Torrico's call for a new law to address defamatory and harassive postings: "With the proliferation of the Internet, chat rooms and social networking sites where people can post anonymous comments, there is this notion that the Web is no holds barred . . . . What I am saying is that there should be some responsibility and repercussions. We should begin to look at these sites. We should be doing whatever we can to protect people's reputations and their safety.").

185. *See, e.g.*, Debra Cassens Weiss, *Justice Breyer and Several Lawyers Were Victims of Data Breach*, A.B.A. J. LAW NEWS NOW, July 9, 2008, http://abajournal.com/news/justice_breyer_and_several_lawyers_were_victims_of_data_breach (finding that while using file-sharing software to trade music or movies, employee of investment firm "inadvertently exposed personal information about 2,000 of the firm's clients. About 700 of the records included Social Security numbers, names and birth dates . . . . "). *See generally* Boeve, *supra* note 101, at 117-18 ("Downloading and sharing music files over the Internet has been in the public eye since the advent of

similar disregard for the rights of others threatens the Internet community at large,[186] and consequently, prioritizing enforcement of legislative initiatives intended to discourage such behavior over specious Internet infringer free speech and privacy claims, is in the best interests of society as a whole. An efficacious response to this problem requires a sober assessment of Internet anonymity in the promulgation of legal mechanisms designed to balance the pertinent property rights and individual liberties. Moreover, it will also require judicial cognizance of the broad social utility challenges attendant to illegal file-sharing conduct, and similar Internet abuse of the rights of others.

---

file sharing software, which allows average music lovers to easily download a digital copy of virtually any song. If the song was copyrighted, then the download was theft; however, most music lovers did not equate the illegal download with shoplifting a compact disc featuring the same song."); Goldsmith, *supra* note 17, at 844 ("As with most technological advances, there is a dark side to the computer revolution. The Internet has made the world both larger and smaller, creating new resources and educational opportunities beyond imagination. But it has also left the courts and Congress with the troublesome task of applying traditional legal doctrines to a complex and constantly evolving mode of communication.").

186. *See, e.g.*, Hawke, *supra* note 168, at 17 ("For many colleges and universities, implementation [of digital information technology] has been successful; in fact, use of computers for communication and research has replaced more traditional modes. But this widespread use has given birth to a new generation of problems for universities that revolve around the potential abuse of the information available on the internet. Copyright issues of intellectual property available online are at the forefront of these concerns, especially since the university must balance the interests of protecting its own information with being a conduit for the access and use of information owned by others. . . . [Moreover, r]egardless of the validity of [individual copyright holder] complaints, colleges nevertheless must devote substantial legal and administrative resources to address this activity."); Lidsky, *supra* note 25, at 903-04 ("The problem, therefore, is to strike a balance between free speech and the preservation of civility. If the goal of making public discourse more participatory and ultimately more democratic is to be realized, the speech of ordinary John Does merits a very wide expanse of 'breathing space,' wider than it currently receives. . . . Although any approach to the problems posed by the new Internet libel actions must respond to the unique culture of the message boards, the law cannot allow that culture to degenerate into a realm where anything goes, where any embittered and malicious speaker can lash out randomly at innocent targets. Although many of the new libel plaintiffs are powerful corporate Goliaths suing to punish and to deter their critics, some are not. Some are simply responding in the only way available to prevent aggressively uncivil speech, the sole purpose of which is to cause emotional and financial harm. Hence, any solution to [these] problems . . . must be tuned finely enough to distinguish incivility that must be tolerated for the good of public discourse from incivility that destroys public discourse." (footnotes omitted)); Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 216 (2003) ("For states to meet their responsibilities in the online world, states must find ways to transpose the powers of enforcement to the internet.").

A. *The Abuse of Internet Anonymity*

While Internet anonymity yields many desirable social benefits, shielding illegal conduct is certainly not one of them.[187]

187. *See, e.g.*, Elektra Entm't Group, Inc. v. DOES 1-9, No. 04 Civ. 2289, 2004 U.S. Dist. LEXIS 23560, at *6-7 (S.D.N.Y. 2004) ("First Amendment protection of anonymous speech, like other kinds of speech, is subject to limits. Most importantly in the present context, the First Amendment "does not protect copyright infringement." (citing Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555-56 (1985)); Sony Music Entm't Inc. v. DOES 1-40, 326 F. Supp. 2d 556, 563 (S.D.N.Y. 2004) ("Anonymous speech, like speech from identifiable sources, does not have absolute protection. The *First Amendment*, for example, does not protect copyright infringement, and the Supreme Court, accordingly, has rejected *First Amendment* challenges to copyright infringement actions."); Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000) (The "Supreme Court . . . has made it unmistakably clear that the First Amendment does not shield copyright infringement"); *see also* DOE I and DOE II v. Individuals, 561 F. Supp. 2d 249, 256 (D. Conn. 2008) (holding that Internet anonymity does not shield defamation conduct); *In re* Ottinger, No. 08-03892, 2008 N.Y. Misc. LEXIS 4579, at *7-8 (Sup. Ct. July 8, 2008) (holding the same); DRATLER, *supra* note 45, § 6.05[1][a] ("In general . . . rights protected by the First Amendment do not extend to anonymous 'speech' consisting of others' copyrighted expression used without their authorization in violation of their copyright. [T]he First Amendment is not a license to trammel on legally recognized rights in intellectual property[,] in part because 'the Framers intended copyright itself to be the engine of free expression[.]' Moreover, as the Supreme Court has affirmed, Congress' will, unless irrational, reigns supreme in the field of copyright, which, after all, has its own special source of constitutional authorization."); Hawke, *supra* note 168, at 17 ("Clearly, a college or university has no legal obligation to defend or accept responsibility for the illegal actions of its students, faculty or staff. Downloading music files without authorization and making those available to others equates to copying and dissemination of a copyrighted work, and violates rights that are exclusive to the copyright owner."); Sandeen, *supra* note 180, at 529 (arguing that Internet anonymity should not be permitted to shield consumer fraud: "One problem is that while the Internet is a forum for increased political and social discourse, it is also a place where false, unreliable, defamatory, fraudulent and offensive messages can proliferate. Unfortunately, at the same time consumers can use the benefits of anonymity and pseudonymity to enhance their privacy, anonymity and pseudonymity can be used to foster criminal activity or shield people from responsibility for their fraudulent statements."). *See generally* H.R. REP. NO. 105-551, pt. 2, at 64 (1998) ("Section 512 does not define what is actionable copyright infringement in the on-line environment, and does not create any new exceptions to the exclusive rights under copyright law. The rest of the Copyright Act sets those rules."). For an argument espousing the benefits of "limited property lawbreaking" in connection with intellectual property rights, see Eduardo Moises Penalver & Sonia K. Katyal, *Property Outlaws*, 155 U. PENN. L. REV. 1095, 1164-65 ("We are concerned that, in its strategies of punishment, the law may aim to preclude too much property lawbreaking. . . . [T]he law must take into account the possible socially productive nature of some property lawbreaking, not just its social costs. In fact, total deterrence does not appear to be the goal of most contemporary theorists. Moreover, at least in practice, the degree and likelihood of punishment for most property law violations have left sufficient play in the joints of the system to permit some kinds of intentional lawbreaking to lead to significant legal change. The dynamically evolving technologies and strategies of law enforcement, however, constantly threaten to remove the needed flexibility within the enforcement

Unfortunately, many Internet users simply don't understand that "cyber-invisibility" is neither inviolable nor legally opaque.[188] The notion that unauthorized file-sharing and similar misconduct is "harmless" if undetected is neither the law nor a valid social more. Moreover, while some Internet advocates characterize illicit file-sharing as a legitimate form of protest,[189] cyber-theft or piracy for

---

of property laws. . . . If too effective at deterring crime, inadvertently harsh (or definite) sanctions can stamp out the information benefits that result from some property lawbreaking. In short, dramatic improvements in the ability to detect and punish property lawbreaking have the ability to shift the potential outlaw's calculus in significant ways, not all of which are socially beneficial. This focus on the possible improvements in the technology of property enforcement to suppress productive lawbreaking is particularly crucial in the context of intellectual property, where the technology (and policy) of property enforcement is presently experiencing revolutionary change.").

188. Kao, *supra* note 11, at 419 ("Internet users have become accustomed to the expectation that their online activities are private; 'many individuals poorly assess the risk of online surveillance and continue to engage in online activities without realizing the risk of exposure.' Perhaps they feel secure because they usually access the Internet from the privacy of their own homes, under the illusion of total anonymity. The assumption is that their identities are private unless there is good cause for them to be revealed." (citation omitted)); *see also* Warner Bros. Records, Inc. v. Souther, No. 1:05CV279, 2006 WL 1549689, at *1, 12-13 (W.D.N.C. June 1, 2006). There, in response to allegations of illegal file sharing, the court observed that:

> [a]ll of the motions now pending before the court have as their genesis defendant's assertion that she did not commit the alleged acts and that if someone else in her home did, she cannot be held liable for such conduct. Defendant also contends that plaintiffs are not entitled to the names and addresses of those others who may have had access to her computer, contending that there exists a federal privilege from disclosing such matters inasmuch as they may involve minors.

Souther, 2006 WL 1549689, at *4. The court concluded that the identities of all persons who had access to defendant's computer is information that plaintiffs are entitled to have. *See id.* The court explained that:

> [c]learly, the identity of the defendant's grandson or of other persons, even if they are minors, who may have used defendant's computer and her ISP to purportedly commit violations of federal copyright laws is well within the bounds of discovery in a copyright infringement action. Such information is made even more relevant where a defendant interposes the possible acts of third parties as a shield to liability. Simply put, plaintiffs have an absolute right to know who may have unlawfully infringed their copyrights, and defendant's failure to provide such information to plaintiffs or properly interpose objections is without legal support.

Id. Facilitating the disclosure of infringing subscriber identities, and ultimately, infringer focused infringement litigation strategies, may well prove a most effective means of copyright public education. *See id.*

189. *See, e.g.*, Sony Music Entm't Inc. v. DOES 1-40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004) ("Arguably . . . a file sharer is making a statement by downloading and making available to others copyrighted music without charge and without license to do so. Alternatively, the file sharer may be expressing himself or herself through the music selected and made available to others."); Jo-Ann Parks, *X-Files, Buffy Fans*

personal gain is no more socially progressive than urban looting in the aftermath of a civic outrage or social justice travesty. Civil disobedience in the cause of social justice is a vital, even hallowed means of personal expression and sacrifice in American society, and it should not be demeaned by comparisons with juvenile or illicit schemes to obtain music or movies for free.

These realities underscore the analytical deficiencies in entreaties which assert that the application of Section 512 Subpoenas to Conduit ISPs would undermine legitimate free speech and privacy rights. As revered as these liberties are in American society, they have never been held to be sacrosanct entitlements, eclipsing all other societal interests.[190] Whatever the particular means of public communication at issue, Congress has always had both the responsibility and the authority to balance the societal stake in open and uninhibited exchange against the national interest in a system of incentives intended to stimulate creative expression.[191] While some laypersons may be misinformed as to the actual breadth of the Constitutional guarantees of free speech and personal privacy, and some legal commentators may simply disagree with the specific free speech/privacy versus copyright balance struck by Congress in

---

Protest Fox, SPACE.COM, June 16, 2000, http://www.space.com/sciencefiction/tv/fanstock_000616.html.

190. *See, e.g.*, *Harper & Row*, 471 U.S. at 555-56; *Sony Music Entm't*, 326 F. Supp. 2d at 567; *Elektra Entm't Group*, 2004 U.S. Dist. LEXIS 23560, at *6-7; *Reimerdes*, 82 F. Supp. 2d at 220; *In re* Subpoena Duces Tecum to Am. On-Line, Inc., No. 40570, 2000 WL 1210372, at *6 (Va. Cir. Ct. Jan. 31, 2000); *In re* Ottinger, No. 08-03892, 2008 N.Y. Misc. LEXIS 4579, at *3 ("The internet is creating emerging legal issues, from jurisdiction to discovery. The identification of anonymous bloggers—posting defamatory statements on the internet—is one of those issues. There is no question that the First Amendment protects the right of a person to speak anonymously. That protection, however, is no greater than that of the right of a person to speak when their identity is known. Anonymous speech is not absolute and does not provide a safe haven for defamatory speech.").

191. *See* Marci A. Hamilton, *Copyright at the Supreme Court: A Jurisprudence of Deference*, 47 J. COPYRIGHT SOC'Y U.S.A. 317, 319 (2000) ("Elements of the [Supreme C]ourt's . . . interpretation of the Copyright Clause . . . include an emphasis on the public good that forces author's rights to be conditioned by the public . . . . From the first case, through the present, the Court has treated copyright law as positive law, the parameters of which are determined by Congress ([as] limited by the Constitution's strictures)."); *see also* McDonald, *supra* note 169 at 542-43 ("Article I, Section 8, Clause 8 of the U.S. Constitution, often called the Copyright Clause, empowers Congress to grant creators a limited monopoly over their works, both as an incentive to and reward for creating new works. In exchange, the public benefits from the dissemination of and access to the work while it is protected and, later, from an enriched and abundant public domain once the copyright expires. Thus, the Copyright Clause facilitates what is, in effect, a social bargain that seeks to achieve what the Framers envisioned as one of the primary goals of copyright: the promotion of learning.").

the DMCA and the Liability Limitation Act,[192] the fact remains that it is within Congress's province to determine the desirable balance of these sometimes competing Constitutional goals.[193] In facilitating

192. *See, e.g.*, Kreimer, *supra* note 20, at 96-98; Okediji, *supra* note 17, at 109-112; Yen, *supra* note 17, at 1888-89 ("The DMCA's safe harbor scheme creates First Amendment problems in three ways. First, it ossifies and perpetuates ambiguities in existing law that encourage ISPs to indiscriminately remove material from the Internet . . . . If the DMCA did not exist, there would likely be future litigation in which courts could clarify and strengthen existing law, thereby reducing uncertainty and the need for ISPs to behave defensively . . . . This will tend to make incentives for indiscriminate removal of material from the Internet a permanent feature of the legal landscape. Second, the DMCA's safe harbor scheme increases the incentive for indiscriminate removal of material by protecting ISPs from actions by their subscribers . . . . As long as ISPs remove material upon the formal request of content providers and follow DMCA procedures, subscribers are barred from recovery. This makes removing contested material from the Internet even more attractive than it already is. Third, the DMCA's safe harbor scheme exacerbates the effect of any mistaken action against speech by effectively circumventing the procedures that would normally protect a copyright defendant from unjustified curtailment of her free speech rights. As noted earlier, subscribers can deny the existence of infringement and thereby prompt ISPs to restore disputed material to the Internet in not less than ten nor more than fourteen business days. However, if the content provider files suit and gives notice of the suit to the ISP before restoration occurs, the ISP must keep the disputed material off of the Internet in order to maintain its safe harbor. As a practical matter, a content provider need only file a lawsuit to get an alleged copyright infringement removed from the Internet pending the outcome of litigation. This is tantamount to awarding the content provider a temporary restraining order and preliminary injunction without any hearing before a court or the posting of a bond." (citations omitted)); McDonald, *supra* note 169, at 560-64.

193. *See, e.g.*, Eldred v. Ashcroft, 537 U.S. 186, 205 (2003). *But cf.* McDonald, *supra* note 169, at 557 (criticizing both the DMCA and the Copyright Term Extension Act, and arguing that Congress may not have struck the proper balance between the interests of copyright holders and that of the public in passing such legislation: "The legislative history reflects Congress' concern to protect and advance the domestic and international economic dominance of U.S. copyright industries. 'When works are protected by copyright, they attract investors who can exploit the work for profit. That in turn brings the work to the consumer . . . .' 'Investors,' 'exploit,' 'profit,' and 'consumer': there is no mention of education, cultural enrichment, or dissemination of ideas."). Similarly, Professor Dratler argues that:

> There is some doubt whether Section 512(h)'s vending machine for subpoenas complies with fundamental notions of constitutional due process insofar as concerns the rights of the Internet user suspected of infringement. To the extent a user of a service provider's system or network has a contractual or other right to privacy or anonymity, that right may be deemed a "property" right or (more likely) a "liberty" interest eligible for protection under the due process clause of the Fifth Amendment to the United States Constitution. If so, the vending-machine procedure would appear to be constitutionally infirm insofar as it adversely affects these interests of the user, for it involves no "due process" for the user's benefit whatsoever.

DRATLER, *supra* note 45, § 6.05[1][c]. Professor Dratler's point is well taken; whereas the copyright law contains "built-in," First Amendment protections, the same cannot be said for "built-in due process protections" and Congress cannot achieve the

copyright holders' access to the identities of alleged infringers, Congress does no more than maintain a constitutionally-mandated equipoise: just as the copyright holder is denied a property right in the ideas embodied in her creative expression, such that these ideas will remain available for unrestricted public discourse, the right of individual speech and exchange ends where the copyright holder's exclusive rights begin.[194]

B. The Balance of Copyright Protection and Internet Subscriber Interests in the Liability Limitation Act

In determining the appropriate balance between intellectual property protection and individual liberty interests, Congress is obviously free to adjust the status quo as necessary to accommodate the realities of new technologies. In this regard, some legal commentators have argued that the purported "ambiguity" in the language of sub-section 512(h) is not merely a by-product of inept draftsmanship, but rather, reflects Congressional sensitivity to the unique nature of Internet discourse, and the need for greater latitude in preserving free speech and privacy interests in this context.[195] In

---

protection of the property rights of copyright holders at the expense of the equally legitimate property interests of private citizens. Whether the Section 512 Subpoena procedure withstands Professor Dratler's observations, however, is beyond the scope of the present article.

194. *See Eldred*, 537 U.S. at 219-21; *see also* Dastar Corp. v. Twentieth Century Fox Film Corp., 539 U.S. 23, 37 (2003); *Harper & Row*, 471 U.S. at 558; Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 164 (1975); 4 NIMMER ON COPYRIGHT § 19E.03[A][2] (2008) ("In general, the democratic dialogue—a self-governing people's participation in the marketplace of ideas—is adequately served if the public has access to an author's ideas, and such loss to the dialogue as results from inaccessibility to an author's 'expression' is counterbalanced by the greater public interest in the copyright system."); Yen, *supra* note 17, at 1866 ("Of course, copyright's effects on free speech do not mean that copyright law is in and of itself unconstitutional. The First Amendment permits certain restrictions on speech, especially when the restrictions promote important public interests and the restricted speech adds little to the free marketplace of ideas. For example, restrictions against false advertising promote the public interest in accurate information about goods and prevent innocent consumers from being cheated. At the same time, the speech being restricted (that is, the false advertising) does little to further the First Amendment's purposes. Similar arguments also support restrictions on obscenity and child pornography, the content of corporate prospectuses, and libelous speech."). Moreover, Congress has also made provision for necessary intrusion upon the author's exclusive rights in her expression, for example, by codifying the Fair Use Doctrine. *See* 17 U.S.C. § 107 (2006).

195. *See, e.g.*, *Verizon III*, 351 F.3d at 1237-38. *See generally* Lidsky, *supra* note 25, at 889-90 ("[Internet] libel suits may chill [Internet discourse] simply by threatening to reveal the identities of those who speak their minds online. . . . [C]orporate plaintiffs easily can make out a prima facie libel claim any time they receive harsh criticism online. Once a complaint is filed, it is a simple matter to get a subpoena to force the ISP to divulge the anonymous defendant's identity. As more and more suits are filed, many Internet users will come to recognize the ease with which their online anonymity

other words, although convinced of the need for subscriber identity disclosure in unauthorized posting cases (which involve Storage ISPs), Congress simply balked at invading the free speech and privacy interests of Internet users engaged in "one-to-one" exchanges (which involve Conduit ISPs).[196]

While this explication of the language of sub-section 512(h) is not without appeal, there are several reasons why it is not a likely depiction of Congress's actual intent. For one thing, it is unsupported by the legislative history to the Liability Limitation Act.[197] Moreover,

---

can be stripped simply by the filing of a libel action, and they will censor themselves accordingly. Such self-censorship is salutary to the extent that it makes Internet users more temperate and more cautious about making unsupported factual assertions. Indeed, the widespread use of pseudonyms online is responsible for many of the abuses perpetrated by Internet speakers. But revelation of identity has negative consequences as well—it may subject the user to ostracism for expressing unpopular ideas, invite retaliation from those who oppose her ideas or from those whom she criticizes, or simply give unwanted exposure to her mental processes. There is some danger, therefore, that the growing popularity of the new Internet libel suits may chill more than defamatory falsehoods--it may also chill the use of the Internet as a medium for free-ranging debate and experimentation with unpopular or novel ideas." (footnotes omitted)).

196. Some privacy advocates hail a recent decision of the European Union as embodying just such a balance of privacy and intellectual property interests, and exemplifying the approach that American courts should take in construing the Liability Limitation Act. *See generally* Productores de Música de España (Promusicae) v. Telefónica de España SAU, (2007) No. C-275/06 (Grand Chamber Court) (Kokott, Advocate General). While a careful reading of the opinion suggests that the decision may not be so much a broad endorsement of Internet privacy rights, but rather, a refusal to permit private intellectual property holders to appropriate broad disclosure mechanisms developed with national security and criminal conduct in mind, in any case, the decision affirms the legislative balancing function in protecting intellectual property rights and privacy interests.

> The protection of copyright is an interest of society, the importance of which has been repeatedly emphasised by the Community. Consequently, even though the interest of rightholders is primarily not of a public, but of a private nature, this aim can be recognised as a fundamental interest of society . . . . It is however not certain that private file sharing, in particular when it takes place without any intention to make a profit, threatens the protection of copyright sufficiently seriously to justify recourse to [disclosure] . . . . *That assessment should—subject to review by the Court—be left to the legislature.* In particular when Member States make the infringement of copyright by file sharing a criminal offence, they undertake a corresponding assessment . . . . Criminal liability would admittedly be weighty evidence of a sufficiently serious threat to the protection of copyright, but criminal law is not necessarily the only form in which the legislature can give expression to an appropriate condemnation. Rather, the legislature can also enforce that assessment by first providing only for communication of personal traffic data in order to enable civil proceedings to be brought."

Id. ¶¶ 105-08 (emphasis added).

197. *See* H.R. REP. NO. 105-551, pt. 2, at 9 (1998); *see also* Boeve, *supra* note 101, at 129 ("Specifically, the history of the DMCA . . . indicates that the subpoena power of

this rationale seems inconsistent with traditional notions regarding the core values which underlie First Amendment protection. For example, an affirmative decision to apply Section 512 Subpoenas to Storage ISPs, but not to Conduit ISPs, would suggest that Congress was more concerned about protecting free speech where one subscriber sends material directly to another subscriber, as opposed to where she posts material as part of a public statement on a website, chat room, or blog. This logic hardly seems consistent with traditional First Amendment analysis and jurisprudence, however, which emphasize the importance of *public* discourse.[198]

On the other hand, the notion that Congress was especially reluctant to encroach upon Internet subscriber "one-to-one" privacy interests provides a stronger basis for the argument that Congress did not intend that Section 512 Subpoenas be applied to Conduit ISPs. It is certainly plausible that Congress might have held the privacy interests of individuals engaged in "one-to-one" communications, as opposed to those who seek to share their views with the public in chat rooms and blogs, in higher Constitutional esteem. As discussed above, however, the privacy inherent in anonymous speech is even more vital to the Internet posting of "public statements," in order to assure the traditional, robust public debate anticipated by the First Amendment.[199] Thus, it seems

---

section 512(h) was intended to gather information from ISPs in a timely manner to end illegal activity."); Ravn, *supra* note 27, at 759 (discussing the legislative histories of House Bill 2180 and Senate Bill 1146); Weiskopf, *supra* note 20, at 49-58.

198. *See generally* Bartnicki v. Vopper, 532 U.S. 514, 533 (2001) ("'The essential thrust of the First Amendment is to prohibit improper restraints on the *voluntary* public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom *not* to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect.'" (quoting Estate of Hemingway v. Random House, Inc., 23 N.Y.2d 341, 348 (1968)); Landmark Commc'n, Inc. v. Virginia, 435 U.S. 829, 838 (1978) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs." (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966)); Lidsky, *supra* note 25, at 893-94 ("From a First Amendment scholar's perspective, the fascination of the Internet lies in its potential for realizing the concept of public discourse at the heart of the Supreme Court's First Amendment jurisprudence. The dominant First Amendment metaphor for describing public discourse is the 'marketplace of ideas.' The marketplace of ideas is a sphere of discourse in which citizens can come together free from government interference or intervention to discuss a diverse array of ideas and opinions. Ideally, the process of interacting in the marketplace of ideas not only fosters the 'search for truth'; it also enables citizens to transcend their differences in order to forge consensus on issues of public concern . . . . Public consensus, in turn, is an essential precondition of democratic self-government. This, at least, is the First Amendment ideal." (footnotes omitted)).

199. Sony Music Entm't Inc. v. DOES 1-40, 326 F. Supp. 2d 556, 562 (S.D.N.Y.

unlikely that Congress would have greater concern for the anonymity of individuals engaged in "one-to-one" exchanges of third-party materials (as distinguished from "one-to-one" exchanges of private statements) than it would have for the anonymity of individuals exposing such material to public scrutiny and debate.

Finally, even setting free speech considerations aside, recognition of a special Congressional concern for the privacy interests attendant to "one-to-one" distributions of copyrighted works does not inevitably lead to the conclusion that Conduit ISPs were intentionally excluded from the ambit of Section 512 Subpoenas. To the contrary, the presence of such concern would explain Congress's decision to require that a 512(c) Notice accompany a Section 512 Subpoena in the first place. Rather than exclude Conduit ISPs altogether, a socially responsible compromise (and one more consistent with the overarching goals of the Liability Limitation Act) would be to require a complaining copyright holder to provide concrete details regarding infringing activity, so as to better assure the receiving ISP (and its subscriber) that the disclosure of the subscriber's identity is being sought in connection with documented wrongdoing, and is not merely a copyright holder "fishing expedition."[200]

2007); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999); *see* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (order requiring association to produce membership list held to violate First Amendment right to speak anonymously and the freedom of association).

200. *See* Dutcher, *supra* note 98, at 511. Professor Dutcher makes a similar argument in connection with the 512(c) Notice requirement that the ISP locate infringing material. *See id.* He explains that:

> A more plausible conclusion [regarding the inclusion of the 512(c) Notice is that, in Congress' attempt] to ensure that individuals received adequate protections against unconstitutional invasions, the added component that the ISP must be able to locate the file in question, was added as a procedural safeguard before a subpoena could issue; if the ISP, looking to the user's shared files, was unable to locate the file in question, or any shared files at all for that matter, it could, on the user's behalf, challenge the subpoena as suspect, or on the grounds that notice was not properly given. Such an interpretation seems to be more consistent with a plain text reading of the statute, practicality and common sense, and, as discussed below, Congress' stated intent that the Act be flexible enough to meet the challenges presented by new technology.

Id. (citation omitted). *See also* Boeve, *supra* note 101, at 142 ("In fact, chapter 512 of the DMCA provides adequate procedural safeguards to protect against improper uses [of the Section 512 Subpoena] that would violate an Internet subscriber's First Amendment rights. These safeguards include the requirement that statements be made with a good faith belief of unauthorized use and that the information is accurate under penalty of perjury. The protections also include penalties for misrepresentations regarding infringing material, including liability for damages and attorney's fees. Another protection requires a sworn declaration that the subpoenas are only sought to obtain the identity of an infringer and 'will only be used for the purpose of protecting

C. *Judicial Balancing of Copyright Protection and Internet Subscriber Interests*

As demonstrated by *Verizon III* and its progeny, even where the legislature affirmatively undertakes to harmonize the relevant Internet constituent interests, unless the courts embrace the overall social balancing scheme, curtailment of Internet abuse of property and personal rights will remain an elusive goal. Some courts have demonstrated the pragmatic sagacity required to attain socially cognizant, commonsense resolutions of these conflicts. For example, recently in *DOE I vs. Individuals*,[201] the United States District Court for the District of Connecticut was confronted with a request for an identity-disclosure subpoena by two female students attending Yale Law School, who had been the subject of malicious statements posted by individuals using cyber-pseudonyms on a law school admissions website.[202] In addition to claims alleging libel, invasion of privacy, and negligent and intentional infliction of emotional distress, because one of the posters posted a photograph of DOE II without her permission, the complaint included a claim for copyright infringement.[203]

The court issued the subpoena, which plaintiffs served on the ISP which provided the Internet connection for one of the posters, known only as "AK47."[204] In response to the subpoena, "AK47" filed a motion to quash, arguing that disclosure of his identity would violate

---

rights' under the DMCA.").

201. 561 F. Supp. 2d 249 (D. Conn. 2008).

202. *Id.* at 251. As described by the court:

> The first message about Doe II that appeared on [the web site] was posted on January 31, 2007, by an anonymous poster. The message linked to a photograph of Doe II and encouraged others to "Rate this HUGE breasted cheerful big tit girl from YLS." After this message was posted, dozens of additional messages about Doe II appeared in the thread. These messages contained comments on Doe II's breasts and the posters' desire to engage in sexual relations with her. Certain of the posters appeared to be Doe II's classmates at Yale Law School because of personal information they revealed. The posts regarding Doe II continued throughout the winter and spring of 2007, and included statements, for example, that she fantasized about being raped by her father, that she enjoyed having sex while family members watched, that she encouraged others to punch her in the stomach while seven months pregnant, that she had a sexually transmitted disease, that she had abused heroin, and that a poster "hope[s] she gets raped and dies." On March 9, 2007, a poster sent an email directly to Doe II and at least one member of the Yale Law School faculty describing the alleged criminal history of Doe II's father.

Id.

203. *Id.* at 252.

204. *Id.*

his First Amendment right to anonymous speech.[205] While acknowledging that the First Amendment does indeed protect anonymous speech, the court also noted that the right to speak anonymously, on the Internet or otherwise, is not absolute and does not protect speech that otherwise would be unprotected.[206] The court then proceeded to evaluate the parties' competing interests, assessing five factors in its effort to strike the proper socio-legal balance: (i) whether the plaintiffs have posted notice of the subpoena, thereby affording the anonymous party an opportunity to object to the disclosure; (ii) whether plaintiffs have set forth the specific, actionable communications made by the anonymous party; (iii) the specificity of the subpoena, the need for the information sought, and the availability of alternative means through which to obtain the information; (iv) the anonymous party's expectation of privacy when she posted her communications; and (v) whether plaintiffs have made an adequate showing of their substantive claims against the anonymous party.[207] Although it concluded that all five factors weighed in favor of the plaintiffs, the court placed the greatest weight on the fifth factor:

> Finally, and most importantly, the Court must consider whether the plaintiffs have made an adequate showing as to their claims against the anonymous defendant.
>
> . . . .
>
> Several courts have required that a plaintiff make a concrete showing as to each element of a prima facie case against the defendant. Under such a standard, "[w]hen there is a factual and legal basis for believing [actionable speech] has occurred, the writer's message will not be protected by the First Amendment." The Court finds such a standard strikes the most appropriate balance between the First Amendment rights of the defendant and the interest in the plaintiffs of pursuing their claims, ensuring that the plaintiff "is not merely seeking to harass or embarrass the speaker or stifle legitimate criticism."[208]

Consequently, faced with a prima facie case of actionable wrong doing, the court denied the motion to quash.[209]

While *DOE I* is not a typical Internet copyright infringement case, it is nonetheless instructive as to the kind of interest weighing

---

205. *Id.* 252-53.

206. *Id.* at 254.

207. *Id.* at 254-55 (citations omitted).

208. *Id.* at 255-56 (citations omitted); *see also* Sony Music Entm't Inc. v. DOES 1-40, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) ("[D]efendants' First Amendment right to remain anonymous must give way to plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.").

209. *Id.* at 257.

that courts should undertake in resolving these disputes.[210] Where there is concrete evidence of illegal conduct, the court should genuinely consider whether important civil liberties are being distorted to shield such conduct. Similarly, in interpreting statutory initiatives promulgated to curtail such activity, courts should keep the relevant social realities in mind. Had the *Verizon III* court employed such an approach in reconciling seemingly competing directives in the language of sub-section 512(h), it is likely that the court would have reached the opposite conclusion as to the reach of the Section 512 Subpoena, and more accurately implemented the objectives of the Liability Limitation Act.[211]

CONCLUSION

By all means, unfettered access to Internet subscriber identities can result in copyright holder abuse.[212] Unchecked subscriber

---

210. *See, e.g.*, Greene, *supra* note 182, at 1180 ("Internet piracy is not merely an enforcement conundrum, but 'a widespread social problem.' As such, litigation against individual copyright infringers seems doomed to fail unless the music industry can inculcate 'copynorms,' a short-hand term indicating, a broad cultural shift in social attitudes toward copyright piracy."); Robert P. Merges, *Locke Remixed(;),* Berkeley Center for Law and Technology (2007), http://repositories.cdlib.org/bclt/lts/30 (arguing that the rights of copyright holders must be considered in assessing the interests of unauthorized "remixers" of copyrighted content).

211. *See, e.g.*, *DOE I,* 561 F. Supp. 2d at 255.

212. *See, e.g.*, Lidsky, *supra* note 25, at 855 ("John Doe has become a popular defamation defendant as corporations and their officers bring defamation suits for statements made about them in Internet discussion fora. These new suits are not even arguably about recovering money damages but instead are brought for symbolic reasons—some worthy, some not so worthy. If the only consequence of these suits were that Internet users were held accountable for their speech, the suits would be an unalloyed good. However, these suits threaten to suppress legitimate criticism along with intentional and reckless falsehoods, and existing First Amendment law doctrines are not responsive to the threat these suits pose to Internet discourse."); Austin Modine, *Oklahoma Woman Takes Sue Happy RIAA to the Bank*, THE REGISTER, July 17, 2007, http://www.theregister.co.uk/2007/07/17/riaa_pays_legal_fees. In connection with evidence of illegal downloading activity, the RIAA obtained the identities of Internet account holder Deborah Foster and her adult daughter. *See* Modine, *supra.* When the RIAA brought suit, Ms. Foster steadfastly denied any knowledge of the activity, whereas her daughter defaulted and judgment was entered against her. *See id.* Nonetheless, the RIAA continued with its suit against Ms. Foster. *See id.* The court not only dismissed the suit against her, but awarded Ms. Foster almost $70,000 in attorneys' fees, doubting that "an internet-illiterate parent, who does not know Kazaa from a kazoo" could be liable for copyright infringement committed by someone else using her internet account." *See id.* The court apparently concluded that having obtained a judgment against the likely culprit, the RIAA was engaging in abusive litigation in pursuing the claims against Ms. Foster. *See id.*; *see also* Molly McDonough, *Oregon 'Ground Zero' in RIAA Battle Against File Sharing*, A.B.A. J. LAW NEWS NOW, Nov. 30, 2007, http://www.abajournal.com/news/oregon_ag_fights_riaa_subpoena (discussing allegations by the Oregon Attorney General that the RIAA's illegal file-sharing

infringement, however, is hardly a socially responsible alternative. A vibrant Internet community requires a realistic assessment, balancing, and protection of all of the competing, legitimate interests.[213] The Copyright Infringement Liability Limitation Act, including its extension of Section 512 Subpoenas to Conduit ISPs, helps to achieve the proper Internet constituent and social utility balance. Properly construed, the Act's statutory scheme appropriately places the principal burden of preventing or redressing Internet subscriber infringement primarily on copyright holders, and on those Internet users who engage in the unauthorized distribution of copyrighted works, and not on ISPs and the rest of the Internet community. Such a construction of the Act promotes responsible, and socially productive, Internet discourse to the collective benefit of the Internet community and society as a whole.

---

investigation methods may be unfair and unlawful).

213. *See, e.g.*, Cynthia M. Ho, *Attacking the Copyright Evildoers in Cyberspace*, 55 SMU L. REV. 1561, 1561-62 (2002) ("In the context of copyrights on the Internet, different evildoers are identified, depending on who is asked to identify the evildoers. For example, to most consumers, the evildoers in cyberspace are the copyright owners that have stripped the Internet of its freewheeling nature by removing things such as the file-sharing tool Napster. On the other hand, major copyright owners vilify consumers—and those who assist them—for making copies of copyrighted material with little regard for whether the consumers own original copies. The identification of evildoers implicitly discounts the possibility that parties merely possess differing, but reasonable views. Rather, the current polarized vision of evildoers has created a situation in which consumers are immune to allegations of copyright piracy and content owners rush to create new methods—whether legal or technological—to halt consumer copying"). Recognizing and reconciling these diverse interests—and the need to view the issues through the lenses of technology, law, economics, psychology and sociology, and public policy—are important first steps in the balancing exercise that is at the heart of the current digital policy debate. *See id; see also* Hawke, *supra* note 168, at 27-28 ("While [addressing] the human component is more challenging to implement, its effect may negate the need for physically restricting access to electronic information-and the continuing march towards more and more regulation. Educating the current and the next generation of students about the ethical use of technology is perhaps the most important approach to resolving this issue. That education needs to go beyond the legalities of using digital information. The prevailing notion—if one has the technical ability to access information, it is acceptable to use it—needs to be dispelled. Users need to be informed that such activity is, at best, unethical and, at worst, unlawful. Those who use computers for communication, entertainment or study need to understand there needs to be a code of behavior online—just as there is in the physical world.").