The DMCA Subpoena Power: Who does it Actually Protect?

by
Thomas P. Ludwig[*]

I. INTRODUCTION

After years of legal maneuvering and courtroom skirmishes, the lines in the war between copyright holders and online copyright infringers have been clearly drawn. This conflict, which is poised to erupt in courts across the country, began decades ago with the birth of the Internet, which gave rise to a previously unparalleled opportunity for the dissemination, sharing, and enjoyment of every conceivable form of human expression. In addition to the benefits it has provided, the Internet also has given rise to copyright infringement on a global scale through the unauthorized posting and sharing of digital files. After years of unsuccessfully battling Internet service providers (ISPs) and file sharing network software distributors, such as Napster and KaZaA, the war against digital copyright infringement may end soon, now that copyright holders are finally taking action directly against the actual infringers. To bring such actions against individual infringers, copyright holders must serve subpoenas on the ISPs pursuant to the Digital Millennium Copyright Act[1] [hereinafter DMCA] to obtain the infringers' subscriber information. Before the real conflict concerning copyright infringement can be fought in the courts or over settlement tables, various issues with the intermediate subpoena process must be resolved. First, does the subpoena authority granted by the DMCA put too much power into the hands of

[*] The author received a B.A. in Mathematical Economic Analysis and Managerial Studies from Rice University and is a candidate for Juris Doctor, class of 2004, at Southern Methodist University Dedman School of Law. He would like to thank Debbie Huang for her support and recommendations during the writing of this article.

[1] Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.). The subpoena provision, which is the focus of this Article, is found in 17 U.S.C. § 512 (2000).

copyright owners? And even more importantly, does this subpoena power strip from alleged infringers any defense that they may have against its abuse? Unless an appropriate balance can be reached with respect to the authority granted by the DMCA's subpoena provision, the war against copyright infringement will be won at the expense of service providers and the Constitutional rights of alleged infringers.

The goal of this Article is to demonstrate that the DMCA subpoena provision neither aids those attempting to enforce copyrights nor sufficiently protects the interests of Internet users. A recent decision by the DC Court of Appeals stripped copyright holders of the use of the DMCA subpoena in situations where the offender's ISP acts merely as a conduit for the transmission of infringing material, which encompasses the most pervasive and egregious form of infringement: unauthorized sharing of copyrighted material via peer-to-peer (P2P) networks, such as KaZaA.[2] Thus, the DMCA subpoena power is unavailable to copyright holders when it is most needed. This situation must be remedied.

At the same time, and even more importantly, additional statutory safeguards protecting the interests of ISPs and the rights of alleged copyright infringers must be built into the subpoena provision, which may be accomplished without sacrificing or significantly impeding copyright owners' ability to enforce their copyrights. At best, the DMCA subpoena provision, in its current form, completely undermines alleged infringers' Fifth Amendment due process rights and unfairly places the likely immense burden of challenging and responding to subpoenas on ISPs. At worst, the provision is susceptible to mistakes and abuse by those who would use it for purposes other than copyright enforcement. The inclusion of certain requirements, such as requiring the provision of notice to alleged infringers before their subscriber information is

[2] Recording Indus. Ass'n of America v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) [hereinafter *Verizon Appeal*].

released, would not unduly burden copyright holders or hinder the enforcement process, but would protect against mistakes and abuse.

Part II of this Article will briefly paint a picture of the events leading up to the copyright holders' utilization of the DMCA subpoena power. Next, Part III will give an overview of the DMCA, focusing primarily on the subpoena provision and Congress's intent regarding that subsection. Part IV will then discuss the specific practical and Constitutional problems that have been raised with respect to the DMCA subpoena power and how the courts have addressed them. Finally, Part V will propose various solutions to the more serious problems and conclude that their implementation would provide a more balanced approach to copyright enforcement.

II. BACKGROUND

A. The Rise of Digital Copyright Infringement

The birth of the Internet granted artists, musicians, and writers the opportunity for global exposure never before achieved through traditional media, such as radio, television, live, books, or compact discs. Ironically, consumers began utilizing the potential for the widespread distribution of copyrighted material via the Internet long before copyright holders or their agents started to take advantage of the possibility.[3] During the 1990's, Internet users began to make copyrighted material publicly available, both legally and illegally, on Web and FTP sites.[4] As technology has since rapidly developed, it has become increasingly simple to reproduce, store, and disseminate copyrighted material as digital files.[5] For example, the processing speed,

[3] Robert MacMillan, *Internet Sparks a Copyright Fire*, Washingtonpost.com (June 24, 2003), *at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A23481-2003Jun23&notFound=true (last visited Feb. 17, 2004).

[4] File Transfer Protocol (FTP) allows the efficient transfer of large files from one remote location to another.

[5] MacMillan, *supra* note 3.

storage capacity, and overall performance of personal computers have grown exponentially during the last twenty years, allowing copyrighted materials to be stored and played in ever increasing levels of quantity and quality.[6] The ability to compress enormous media files while retaining the quality of the original has made the transfer and storage of large amounts of copyrighted material, such as songs and movies, progressively more efficient.[7] Today, even the most inexperienced computer user can engage in copyrighted file sharing with the recent development of P2P networks, which allow users to locate and transfer files directly amongst themselves without the need for intermediate, centralized hubs or servers.[8]

The development of P2P networks and similar file sharing technology has probably had the most significant effect on digital copyright infringement. Currently, there are more than 57 million American users of file sharing technology who, together with millions of other users around the world, are downloading billions of music files every year.[9] At any given time,

---

[6] Raj Sardesai & Michael J. Ram, *Protecting Intellectual Property Rights in Software: The Software Patent*, 11 LOY. CONSUMER L. REV. 99, 99 (1999).

[7] Michael Yang & Francis J. Gorman, *What's Yours is Mine*, 36 MD. B. J. 24, 31 (2003) ("The most popular and well-known format for music compression is known as MP3. The MP3 compression format permits a CD-quality digital music file to be compressed to roughly one-tenth the original size without noticeably affecting the sound quality. With this degree of file compression, the MP3 format allows users to save significant space on their computers and significantly increases the portability of music files. Before compression formats such as MP3 existed, digital music files could not easily be transferred due to their size and the relatively slow speed of most computer data connections. Now, such transfers are able to happen quickly and easily due to the significantly compressed file sizes and the proliferation of ever faster data networks.").

[8] *Id.* at 31-32. *See also* GES Systems, Inc., Networking ("In Peer-to-Peer networks, the connected computers have no centralized authority. From an authority viewpoint all computers are equal. In other words they are peers."), *at* http://www.gessystems.com/networking.htm (last visited Feb. 17, 2004). The following analogy paints a simple description of P2P networks: connecting to another computer via a P2P network is similar to communicating through two-way radios, while traditional networks are more akin to communicating over the phone, which requires the phone company to act as a central hub or server.

[9] MacMillan, *supra* note 3 (citing a study that estimated that more than 5 billion music files were downloaded from P2P networks in 2002). In its recent motion to enforce a subpoena issued to Massachusetts Institute of Technology, however, the Recording Industry Association of America (RIAA) claimed that "[m]ore than 2.6 billion infringing music files are downloaded *monthly*." Motion to Enforce Subpoena Issued to the Massachusetts Institute of Technology at 2, In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MS-00265 (filed Aug. 1, 2003) (citing L. Grossman, *It's All Free*, Time, May 5, 2003, at 60-69) [hereinafter Motion to Enforce Subpoena to MIT].

roughly 700 to 900 million files are available on the infamous KaZaA network alone.[10] Studies show that approximately 90% of the content shared on P2P networks is copyrighted material disseminated without authorization.[11] Based on this 90% infringement rate, there are between 630 and 810 million infringing files available just on KaZaA at any particular moment. KaZaA, however, is not the only P2P network that is being used to share copyright infringing files.[12]

The explosive growth in computer and data transfer technology, especially the development of P2P networks, has fueled the rampant unauthorized dissemination of copyrighted material online.[13] Naturally, this infringement has had a dramatic impact on the profits of many copyright owners, most notably those in the music recording industry. Recent statistics demonstrate the considerable extent of this impact. P2P networks began to take hold late in 1999, and compact disc sales fell immediately, declining 7% in 2000, 10% in 2001, and 11% in 2002.[14] This annual decline in CD sales over the last three years represents more than $1 billion in lost annual revenues.[15] Clearly, the unauthorized sharing of music files on P2P networks is

---

[10] Leander Kahney, *Buck a Song, or Buccaneer?*, Wired News (Oct. 21, 2003) (citing Eric Garland, CEO of BigChampagne, a Beverly Hills, California-based research firm that tracks file-sharing networks), *at* http://www.wired.com/news/business/0,1367,60901,00.html?tw=wn_tophead_1 (last visited Feb. 17, 2004).

[11] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001).

[12] While KaZaA is the most downloaded program on the Internet (over 230 million copies have been downloaded), there are other highly popular P2P network programs in existence, as well. Napster was probably the best known of all the P2P networks, but the RIAA was able to force it to shut down in 2001. Today, Grokster, Morpheus, Lime Wire, and BearShare all operate based on software similar to that used for the KaZaA network.

[13] In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter, 257 F. Supp. 2d 244, 265-66 (D.D.C. 2003) (citing United States v. Elcom, Ltd., 203 F. Supp. 2d 1111, 1132 (N.D. Cal. 2002), the court noted that "[t]he extent of copyright infringement and piracy of intellectual property over the Internet…is well-recognized and 'has reached epidemic proportions.'").

[14] Motion to Enforce Subpoena to MIT at 3 (citing the RIAA's website at http://www.riaa.com/pdf/2002yrendshipments.pdf).

[15] David McGuire, *Online Piracy Frightens Movie Moguls*, Washingtonpost.com (June 24, 2003) (noting that revenues from CD sales dropped from $13.2 billion in 2000 to $12 billion in 2002), *at*

having a substantial effect on the music industry's revenues, and the problem is only getting more serious.[16]

The music industry, however, is not the only market sector feeling the squeeze that widespread copyright infringement is putting on profits. A recent study found that 8 percent of American Internet users illegally downloaded at least one movie during a three-month period in 2002, which is not insignificant considering the number of Internet users in the United States.[17] And while the motion picture industry's estimate of 400,000 illegal movie downloads per day may seem relatively small compared to the many millions of infringing music files downloaded daily, rapid technological development could cause that number to skyrocket within a few years.[18] The software industry is also facing similar issues regarding copyright infringement.[19]

B. Copyright Owners Fight Back

Of course, the music industry and other copyright owners have not given up these lost revenues without a fight, both on the technological and legal fronts. Copyright owners have attempted to protect their interests with new security tools, such as encryption and other copy-protection measures. This strategy has had only limited success, however, due to the rapidly

---

http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A23575-2003Jun23&notFound=true (last visited Feb. 17, 2004).

[16] Motion to Enforce Subpoena to MIT at 3.

[17] MacMillan, *supra* note 3.

[18] McGuire, *supra* note 15. "To date, the size (huge) and quality (poor) of most of the pirated movies and television shows available online have dampened their popularity among casual "peer-to-peer" file swappers. The same high-speed Internet customer who downloads dozens of digital-quality songs every hour may have to wait several hours to get one grainy, cheaply recorded copy of the latest Hollywood release." *Id.* Increases in bandwidth and digital technology, however, could put the movie industry in the same position as the music industry within 3-5 years. *Id.*

[19] MacMillan, *supra* note 3.

evolving nature of technology.[20] Developing new copyright protection systems is an expensive process and technologically sophisticated users are commonly able to circumvent such measures.[21] To make matters worse, the methods of circumvention are generally shared over the Internet with less savvy users.[22]

Copyright owners have not had much more success on the legal front, or at least not until now. Their difficulty up to this point has been finding a party to hold responsible for the unbounded copyright infringement that is taking place. Copyright owners have been extremely wary of directly pursuing individual infringers for fear of creating bad publicity and alienating consumers.[23] ISPs have not been effective targets because Title II of the DMCA, which is the focus of this Article, limits the liability of unwitting service providers in cases involving their subscribers' digital copyright infringement.[24] In addition, service providers have little control over their subscribers' unauthorized downloading of copyrighted material.

While the creators and distributors of P2P network software would appear to be appropriate defendants in actions for contributory or vicarious infringement, the courts' holdings have fallen on both sides of this issue.[25] Although copyright holders will likely continue to fight

---

[20] Martin F. Halstead, *The Regulated Become the Regulators: Problems and Pitfalls in the New World of Digital Copyright Legislation*, 38 TULSA L. REV. 195, 224 (2002) (noting that current copyright protection systems are not effective).

[21] *Id.*

[22] *Id.* In addition, copyright protection systems are extremely controversial and unpopular because they prevent many forms of fair use as well as allow infringement.

[23] Jennifer Norman, Note, *Staying Alive: Can the Recording Industry Survive Peer-to-Peer?*, 26 COLUM.-VLA J.L. & ARTS 371, 392 (2003).

[24] 17 U.S.C. § 512 (2000).

[25] *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029 (C.D. Cal. 2003) (holding that the copyright owners could not obtain relief for contributory or vicarious infringement against the distributors of P2P network software because they did not materially contribute to the infringement once they obtained actual knowledge of it—by the time the distributors became aware of the infringement, there was nothing that could be done to stop it); *but see* In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003) (affirming the preliminary

P2P network software distributors with increasing success,[26] the very nature of P2P networks prevents copyright owners from effectively enjoining their creators to stop the sharing of infringing material.[27] Typically, P2P networks do not operate from central servers that can be shut down or controlled.[28] Once a user downloads the network software, he or she shares files directly with other users outside of the control of the network creators. A victory in the courtroom obtaining an injunction against operation is meaningless if it cannot be enforced. Thus, copyright owners have been forced into a corner with only one way to fight out. They cannot attack the parties enabling the online copyright infringement, so they must directly pursue the actual infringers. As inefficient and distasteful as suing its own consumers for infringement may be, the RIAA announced on June 25, 2003, that it would begin bringing actions directly against the most "egregious infringers."[29]

C. Identifying Individual Infringers

---

injunction entered against Aimster by the district court, concluding that the copyright owners were likely to succeed against Aimster on the basis of contributory infringement) *and* Kazaa/Buma-Stemra, Hof, Amsterdam, 28 maart 2002, rolnr. 1370/01 (holding that KaZaA is acting unlawfully by making software available that allows users to download music files and must shut down or pay $40,000 (US) per day in fines). *See also* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (holding that where a technology is capable of non-infringing uses, the distributor of the technology will not be contributorily liable).

[26] It is becoming less difficult for copyright owners to establish that P2P network operators have actual knowledge of their users' copyright infringement.

[27] Yang & Gorman, *supra* note 7, at 32; Alan B. Davidson, Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace, Prepared Statement before the Senate Committee on Commerce, Science, and Transportation (Sept. 17, 2003) ("Widespread use of the current generation of peer-to-peer programs, which do not include centralized servers, has forced copyright holders to go after infringing users themselves."), *at* http://www.cdt.org/testimony/030917davidson.shtml.

[28] Yang & Gorman, *supra* note 7, at 32. The Napster network, which was not truly P2P, "did require centralized servers in order to catalog all of the information residing on all of its individual users' computers." *Id.* Thus, following its successful lawsuit against Napster, the RIAA was able to force the network to shut down in the summer of 2001. *Id.* KaZaA and the other P2P networks that have sprung up in its place, however, are much more decentralized and virtually impossible to shut down. *Id.*

[29] *RIAA Responds to Senator's Inquiry, Says P2P Users Should Expect Low Privacy*, 8 ELECTRONIC COM. & L. REP. No. 32, at 794-95 (Aug. 20, 2003) [herinafter *RIAA Responds*] (citing an Aug. 14, 2003 letter from the RIAA to Sen. Norman Coleman).

Before copyright owners can sue any alleged infringers, they have to know whom to sue. Copyright owners, such as the Recording Industry Association of America (RIAA), employ agencies that use programs, known as "rangers" or "bots," to search the shared files of computers logged into P2P networks for infringing files.[30] According to the RIAA, "The software then downloads a sample of the infringing files, with date and time of access, and stores the user's Internet Protocol (IP) address."[31] These programs also record the names of all the infringing files that they find.[32] The RIAA claims that its employees manually review and verify the information collected by the search programs before taking any action.[33] Because P2P network users operate anonymously, copyright owners are not able to directly obtain the user's name, address, or other identification information. The IP address, however, enables the copyright owner to identify the user's service provider, which does possess that information.[34] Thus, to obtain a user's subscriber information, the copyright owner must subpoena the service provider pursuant to Section 512(h) of the DMCA.[35] The subpoena process itself will be discussed in greater detail below.

[30] Matthew V. Skelton, *The* Verizon *Cases: A First Look at the Subpoena to Identify an Infringer Under the Digital Millennium Copyright Act*, 5 VA. INTELL. PROP. L. NEWSLINE No. 2, at 5 (June 2003), *available at* www.vsb.org/sections/ip/Newsline%20June%202003%20FINAL.pdf.

[31] Jay Lyman, *RIAA Details Subpoena Strategy*, E-Commerce Times (Aug. 19, 2003), *at* http://www.ecommercetimes.com/perl/story/31372.html (last visited Feb. 17, 2004).

[32] Skelton, *supra* note 30, at 5.

[33] Lyman, *supra* note 31.

[34] *Id.*

[35] 17 U.S.C. § 512(h).

Since announcing its latest strategy in June 2003, the RIAA has served well over 2,000 DMCA subpoenas, at an average of 75 per week.[36] Although service providers received only a limited number of subpoenas from copyright owners before this recent onslaught and responded to each of them without challenge,[37] several providers have reacted to this new trend with motions to quash.[38] Naturally, ISPs are extremely reluctant to freely release subscriber information on a large scale because such a response could drive away consumers.[39] Service providers are also concerned about the potentially enormous administrative and legal costs that would be associated with complying with a flood of such subpoenas if other copyright owners were to follow the RIAA's approach.[40] In these cases, which will be discussed further below, the service providers have challenged the use of the subpoena provision on various statutory, constitutional, and policy grounds with varying success. Somewhat unusually, consumer rights organizations and privacy advocates have aligned themselves with the service providers in challenging the DMCA subpoena provision, albeit certainly with different motives. In any event,

[36] *RIAA Responds*, *supra* note 29, at 795. Based on these subpoenas, the RIAA filed a first wave of 261 lawsuits against individual file sharers on September 8, 2003.

[37] Farhad Manjoo, *AOL's Jekyll and Hyde Act*, Salon Technology & Business (Feb. 10, 2003), *at* http://www.salon.com/tech/feature/2003/02/10/aol_file_sharing/print.html (last visited Feb. 17, 2004). According to Matthew Oppenheim, RIAA's vice president of business and legal affairs, the RIAA had only issued 96 § 512(h) subpoenas since the passage of the DMCA before Verizon became the first ISP to challenge one. *Id.*

[38] In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter, 240 F. Supp. 2d 24 (D.D.C. 2003) [hereinafter *Verizon I*]; In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter, 257 F. Supp. 2d 244 (D.D.C. 2003) [hereinafter *Verizon II*]; In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MC-10209-JLT (Aug. 7, 2003); In re Subpoena to Boston College, No. 1:03-MC-10210-JLT (Aug. 7, 2003); Pacific Bell Internet Servs. v. Recording Indus. Ass'n of America, No. C 03-3560 SI (N.D. Cal. filed July 30, 2003); In re Charter Communications, Inc., Subpoena Enforcement Matter, No. 4:03MC00273CEJ (E.D. Mo. filed Sept. 23, 2003). In addition, several individual users have filed Jane Doe actions against the RIAA challenging the DMCA subpoena provision and its interpretation by the RIAA.

[39] Manjoo, *supra* note 37.

[40] *District of Columbia Court Lacks Authority to Issue DMCA Subpoenas to Boston Schools*, 66 ELECTRONIC COM. & L. REP. No. 1634, at 459 (Aug. 15, 2003).

until these issues with the subpoena provision are resolved, the process of pursuing individual infringers will not be a smooth one for copyright owners.

III. THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. Overview and Purpose of the DMCA

Congress enacted the DMCA in 1998 to "facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[41] Title I of the DMCA, which is not the focus of this Article, amended the Copyright Act[42] to implement two recent World Intellectual Property Organization (WIPO) treaties, "bringing U.S. copyright law squarely into the digital age…"[43] Title II was enacted to introduce a level of certainty with respect to ISPs' potential liability for the online copyright infringement of their subscribers.[44] It attempts to achieve this goal by clarifying exactly when a service provider is liable for its subscribers' transmission or storage of infringing material on its systems and what remedies copyright owners have in such situations.[45] In addition, Title II endeavors to help ensure the growth and efficiency of the Internet and protect the interests of copyright owners by "preserv[ing] strong incentives for service providers and copyright owners

[41] S. REP. NO. 105-190, at 1-2 (1998).

[42] 17 U.S.C. §§ 501 et seq. (2000).

[43] S. REP. NO. 105-190, at 2 (discussing the implementation of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty).

[44] *Id.*

[45] *Id.*

to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[46]

The enacted version of Title II came about largely as a result of lengthy negotiations between representatives of the major copyright owners and officials from the leading ISPs.[47] When the DMCA was first proposed, it originally held service providers liable anytime one of its subscribers posted infringing material.[48] Service providers were able to negotiate a compromise, however, whereby they would not be held liable for unwittingly hosting or transmitting infringing material for their subscribers, as long as they cooperated with copyright owners in combating infringement through various prescribed means.[49]

Title II amended chapter 5 of the Copyright Act[50] to include a new section entitled, "Limitations on liability relating to material online."[51] As its name suggests, section 512 expressly limits the liability of an ISP in specific situations where subscribers use its facilities to commit acts of copyright infringement.[52] In subsections (a) through (d), section 512 provides service providers with "safe harbors" from direct, vicarious, and contributory liability for four categories of activities involving infringement by users: (a) where the ISP merely acts as a

---

[46] *Id.* at 37.

[47] *Id.* at 9. "Title II…reflects 3 months of negotiations supervised by Chairman Hatch and assisted by Senator Ashcroft among the major copyright owners and the major OSP's and ISP's."

[48] Jason Krause, *Caught by the Act: Judge Rules ISPs Must Name Clients Who Trade Copyrighted Material*, 2 A.B.A. J. E-Report 2 (2003).

[49] *Id.*

[50] 17 U.S.C. §§501 et seq. (2000).

[51] *Verizon I*, 240 F. Supp. 2d at 26-27; 17 U.S.C. § 512. This section is the heart of Title II and the source of the DMCA subpoena provision.

[52] *Verizon I*, 240 F. Supp. 2d at 27.

conduit for the transmission of infringing material;[53] (b) where the ISP's system is used for the intermediate or temporary storage of infringing material ("system caching");[54] (c) where the ISP hosts (stores online) infringing material on its servers at the direction of users;[55] and (d) where the ISP refers or links users to the online location of infringing material via directories, index references, hypertext links, and other tools.[56] In order to qualify for the immunity offered by these safe harbors, however, service providers must satisfy certain prescribed conditions, depending on which safe harbor is being claimed.[57] For example, each of these four provisions essentially requires that the ISP have no actual knowledge of the infringing nature of the material at issue.[58] Also, the service provider must terminate the accounts of subscribers engaging in repeat copyright infringement and must inform its subscribers of this policy.[59] In addition to satisfying these conditions and others, service providers must cooperate with copyright owners in their efforts to enforce their copyrights. Section 512 provides copyright owners with two powerful statutory weapons for use in their fight against online infringement, both of which require the cooperation of service providers to be effective: takedown notices[60] and subpoena

[53] 17 U.S.C. § 512(a).

[54] § 512(b).

[55] § 512(c).

[56] § 512(d).

[57] Norman, *supra* note 23, at 392.

[58] *See* § 512(a)(1)-(2) (requiring that the transmission of the infringing material be initiated by a person other than the ISP and that the transmission be "carried out through an automatic technical process"); § 512(b)(1)(A)-(B) (same); § 512(c)(1)(A) (requiring that the service provider not have actual knowledge that the material or activity is infringing); § 512(d) (same).

[59] § 512(i)(1)(A).

[60] § 512(c)(3).

authority.[61] Although this Article focuses primarily on the latter tool, a discussion of the former is pertinent here for purposes of later comparison and understanding the overall structure of section 512.

B. The DMCA Takedown Provisions

Once a copyright owner discovers infringing material online in the manner described previously in Part II, it may issue a takedown notice to the appropriate ISP to "remove or disable access to" that material being made available by its subscriber, who is identifiable by his or her IP address.[62] The requirements for a takedown notice are delineated in the safe harbor provision for ISPs unknowingly hosting infringing material on their servers, section 512(c).[63] It must include the following:

> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party…

---

[61] § 512(h).

[62] § 512(c)(3)(A)(iii). *See also* § 512(b)(2)(E) (requiring the removal of infringing material from system cache upon notification by the copyright owner); § 512(c)(1)(C) (requiring the removal of infringing material from the ISP's system or network upon notification by the copyright owner); § 512(d)(3) (requiring the removal of links or references to the location of infringing material upon notification by the copyright owner). Obviously, there is no takedown provision for infringing material that merely passes through the ISP's system or network, although many copyright holders have even issued takedown notices in such situations as well.

[63] § 512(c)(3).

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.[64]

Delivery of a takedown notice must occur through the service provider's "designated agent."[65] In order for a service provider to qualify for liability protection under one of the four safe harbor provisions, it must designate an agent to receive such takedown notifications, as well as subpoenas.[66] The service provider must make the designated agent's contact information available to the public, both on its website and through the Copyright Office.[67] Clearly, the purpose of this provision is to streamline the delivery process to the greatest extent practicable, ensuring that the enforcement of the takedown notice is prompt and expeditious.[68]

Upon receiving a substantially compliant takedown notice, the service provider must "remove or disable access to" the infringing material.[69] If the service provider wishes to avoid possible liability for directly removing or disabling access to allegedly infringing material residing on its system, it must "take reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material."[70] If the service provider subsequently receives a

[64] § 512(c)(3)(A).

[65] § 512(c)(2).

[66] *Id.*

[67] *Id.* This contact information must include the name, address, phone number, and e-mail address of the agent. § 512(c)(2)(A).

[68] Many service providers, such as Verizon, Pacific Bell, and Comcast, are extremely large corporations with a number of administrative centers around the country. This provision avoids loss and delay by ensuring that each takedown notification goes to the same location and is handled in the same manner.

[69] § 512(c)(1)(C).

[70] § 512(g)(2)(A).

counter notification from the subscriber that the allegedly infringing material was removed as a result of mistake, it must promptly provide the copyright owner with a copy of the counter notification and inform the copyright owner that it will replace the removed material in 10 business days unless the copyright owner pursues a court order restraining the subscriber from engaging in infringing activity.[71] If the copyright owner does not alert the service provider that it has filed such an action, then the service provider must replace the removed material between 10 and 14 business days following the receipt of the counter notification from the subscriber.[72]

With the fairly recent development of P2P networks, ISPs now commonly receive takedown notices pertaining to infringing material *not* residing on their systems or networks.[73] In this situation, which is governed by the subsection (a) safe harbor provision, the ISPs merely act as conduits for the transmission of the infringing material.[74] Thus, they cannot directly "remove or disable access to" the offending files.[75] Section 512 does not explicitly state how this issue should be resolved, and the DC Circuit Court of Appeals recently held that takedown

---

[71] § 512(g)(2)(B)-(C). The counter notification must include the following information:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number…

§ 512(g)(3)(A)-(D).

[72] § 512(g)(2)(C).

[73] *See e.g.*, Bob Sullivan, *Hollywood Gets Tough on Copying*, MSNBC (July 12, 2003) (noting that the MPAA serves approximately 2,000 takedown notifications each week on ISPs for infringement taking place on P2P networks), *at* http://msnbc.msn.com/id/3078567/ (Feb. 17, 2004).

[74] § 512(a).

[75] *Verizon Appeal*, 351 F.3d 1229, 1235 (D.C. Cir. 2003).

notices cannot properly be issued in this situation.[76] At least until this opinion was delivered, however, ISPs generally cooperated with copyright holders in this situation by warning the offending subscriber that if he or she did not expeditiously remove the infringing material, his or her Internet connection would be disabled.[77]

This takedown process contains several important safeguards, which protect both the service provider from liability and the subscriber from improper takedowns. These safeguards are important to note for the sake of comparison because some are strangely lacking from the subpoena provision. First, the copyright owner must include in the takedown notice the required information listed above, which allows the service provider to verify its accuracy.[78] If the takedown notification is not substantially compliant with these requirements,[79] the service provider is not treated as having knowledge of the claimed infringement and, thus, does not have to remove or disable access to the allegedly infringing files.[80] These requirements for the notification are important because they allow the service provider to independently verify that the subscriber is indeed making infringing material available online. As will be discussed shortly, these notification requirements must also be satisfied before a copyright owner can

[76] *Id.* at 1231.

[77] *See* Sullivan, *supra* note 73; Manjoo, *supra* note 37; *Verizon Appeal*, 351 F.3d at 1232.

[78] *See supra* note 64 and accompanying text (quoting § 512(c)(3)(A)).

[79] *See* § 512(c)(3)(B)(ii) (defining substantial compliance).

[80] § 512(c)(3)(B)(i) ("a notification…that fails to comply substantially with the provisions of subparagraph (A) shall not be considered…in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent."); § 512(c)(1)(A)(iii) (stating that the ISP must only remove or disable access to allegedly infringing material upon obtaining knowledge or awareness of the infringement).

obtain a subpoena from the clerk of the issuing court, and is one of the few significant statutory safeguards in the subpoena process.[81]

Second, the procedure for notification and takedown provided in section 512 affords Internet users' interests in making files and material available online with adequate due process protection from possible mistakes or abuse on the part of copyright owners. As just described, the requirements for the notification itself allow the service provider to act as the first line of defense against improper takedown notices. Additionally, takedowns require the provision of actual notice to subscribers.[82] If the service provider removes or disables access to allegedly infringing material residing on its system, it must take reasonable steps to provide prompt notice to the subscriber.[83] If the allegedly infringing material does not lie within the direct control of the service provider, as in the case of files shared on P2P networks, the service provider's warning to the subscriber to personally remove the infringing files obviously serves the same notice function. Such notice provides the subscriber with an opportunity to evaluate and possibly challenge the infringement allegation. The subscriber is in the best position to know whether the relevant files are indeed infringing and to supply evidence if they are not.[84] Thus, common sense suggests that the subscriber should be given actual notice of infringement claims and the removal of allegedly infringing files. There is, however, no such notice requirement for the subpoena provision.

---

[81] § 512(h)(2)(A).

[82] § 512(g)(2)(A).

[83] *Id* Due to the extremely short time period that subscribers are given to respond to this notice (less than 10 days after the takedown), such notice must probably be delivered within 24 hours to be considered effective. Note that this notice requirement does not prevent service providers from giving notice to subscribers *before* taking down the allegedly infringing material, as long as the material is taken down promptly.

[84] Davidson, *supra* note 27.

Third, section 512 provides subscribers with two types of statutory remedies in the event of an improper takedown. The first remedy imparts users with a cause of action against "any person who knowingly materially misrepresents…that material or activity is infringing…"[85] A copyright holder making such a misrepresentation is liable for monetary damages, including costs and attorneys' fees.[86] The availability of this cause of action prevents copyright owners from abusing the takedown provision and non-copyright owners from using it merely for purposes of harassment.

Section 512 also implies that subscribers may bring a cause of action against service providers that improperly remove allegedly infringing material from their systems or networks.[87] Subsection (g) states that service providers will not be held liable for damages resulting from removing infringing material from their systems, regardless of whether the material is infringing, so long as they adhere to the procedure outlined above.[88] By implication, if a service provider does not comply with this procedure in removing allegedly infringing files from its systems or networks, the effected subscriber may realize a cause of action. This provision gives service providers incentive to protect the interests of their subscribers, helps to ensure that service providers will deal with claims of infringement in a fair and consistent manner, and grants subscribers recourse with respect to improper takedowns. Together these two statutory remedies provide users with protection from a broad range of abuse and impropriety with respect to the

[85] § 512(f)(1).

[86] § 512(f). This section cuts both ways, however, since a copyright owner may also sue a subscriber for damages based on misrepresentation in a counter notification that material was removed or disabled by mistake or misidentification. § 512(f)(2). A service provider may also recover any damages incurred as a result of a misrepresentation by a copyright owner or subscriber. *Id.*

[87] § 512(g).

[88] § 512(g)(1).

takedown process. While the first remedy may also be available to those whose subscriber information is subpoenaed based on misrepresentation, the second remedy clearly only applies to the takedown process.

In addition to these built-in safeguards, the takedown provisions promote efficiency in the enforcement of copyrights. The multi-step process for removal of allegedly infringing material tailors itself to the needs and issues of the individual situation and continues only as long as is necessary for the resolution of the conflict. The process also preserves efficiency by providing for short deadlines and automatic, yet reversible, action. If the subscriber or copyright owner does not respond to the notification or counter notification, respectively, that party's concession to the takedown or reposting is assumed. For example, if a copyright owner mistakenly identifies a subscriber's file as infringing, there is no need for a lengthy challenge process or an injunction filing. Such a problem is easily resolved with a simple counter notification from the subscriber to the copyright owner.[89] On the other hand, when the online material is clearly infringing, the subscriber may simply concede its removal without taking any action at all, thus maximizing efficiency.[90]

The takedown process also efficiently resolves the rarer, more complicated situations that involve less clear-cut issues of copyright infringement. The procedure allows for the efficient production of evidence from both sides through the notification and counter notification

[89] § 512(g)(2)(B). If the takedown notice was obviously issued by mistake, the evidence provided in the counter notification would almost certainly resolve such an error (assuming the mistake slipped past the ISP's initial screening of the takedown notice in the first place).

[90] *Id.* If the subscriber does not promptly respond with a counter notification, the removed material is assumed to be infringing and remains offline.

provisions,[91] and if the parties themselves cannot resolve the conflict, the procedure allows the parties to bring it before the court in an injunction proceeding.[92]

This efficiency is extremely important within the context of online copyright enforcement. Due to the rapid manner in which copyrighted works can be copied and distributed worldwide, it is crucial to the interests of copyright holders that infringing files be removed from the Internet as expeditiously as possible.[93] With the vast number of Internet users worldwide, the existence of a single infringing file on a P2P network can have major repercussions for its copyright holder as it is disseminated in an exponential fashion.[94] The large number of Internet users and the epidemic levels of infringement also create the potential for an explosion in the number of copyright enforcement actions brought by copyright owners. With so much infringement occurring, it is essential to all parties involved that the method for dealing with it be as fast and efficient as possible. A cumbersome enforcement system might bottleneck at various points in the process and cause undue delays. Efficiency is also a concern for a subscriber who has had material mistakenly removed from the Internet. Oftentimes, such removed material is significant to the subscriber's website or business, and if it is non-infringing, it should be replaced with all reasonable promptness. Although the takedown provision has already begun to significantly burden ISPs, which must scramble to promptly respond to many notices at one

[91] §§ 512(c)(3), (g)(3).

[92] § 512(g)(2)(C).

[93] *Verizon I*, 240 F. Supp. 2d at 35 (citing S. REP. NO. 105-190, at 8).

[94] Motion to Enforce July 24, 2002 Subpoena Issued by this Court to Verizon Internet Services, Inc. and Memorandum in Support Thereof at 5, *Verizon I*, 240 F. Supp. 2d 24 (D.D.C. 2003).

time,[95] the procedures laid out in section 512 effectively promote the important goals of efficiency and expediency.

C. The DMCA Subpoena Provision

Although arguably more powerful in effect, the subpoena provision in the DMCA is actually somewhat secondary to the takedown notification provisions in at least two respects. First, the subpoena provision has been and still is utilized with much less frequency.[96] The issuance of a subpoena implies more extreme consequences than the more passive issuance of a takedown notification, and such a step is generally taken in anticipation of bringing some type of legal action. Currently, subpoenas are only being issued for the subscriber information of the more flagrant copyright infringers.[97] Second, DMCA subpoenas must be served "piggybacked" on takedown notifications. As will be described shortly, a copyright owner must serve the appropriate ISP with a takedown notification either prior to or simultaneously with its service of the subpoena for the infringer's subscriber information.[98] The fact that the subpoena provision is, in certain respects, secondary to the takedown provisions is significant in shedding light on how Congress intended it to be used.

---

[95] *See* Skelton, *supra* note 30, at 6.

[96] *See* Sullivan, *supra* note 73 (stating that the MPAA, by itself, issues approximately 2,000 takedown notices each week). Before the RIAA introduced its new strategy in June 2003, only a very small number of subpoenas were issued relative to takedown notifications. *See* Manjoo, *supra* note 37 (noting that the RIAA had only issued 96 section 512(h) subpoenas since the passage of the DMCA before Verizon began its challenge). Even now, the RIAA has only issued a few thousand subpoenas since launching its massive campaign and the subpoenas are being issued in conjunction with takedown notifications. *RIAA Subpoenas Halted*, Electronic Frontier Foundation (Dec. 1, 2003), *at* http://www.eff.org/IP/P2P/riaasubpoenas/ (last visited Feb. 17, 2004).

[97] *RIAA Responds*, *supra* note 29.

[98] 17 U.S.C. § 512(h)(5) (2000) ("Upon receipt of the issued subpoena, *either accompanying or subsequent to* the receipt of a [takedown] notification…, the service provider shall expeditiously disclose to the copyright owner…the information required by the subpoena…regardless of whether the service provider responds to the notification.").

The authority to obtain and serve a subpoena under the DMCA is found in section 512(h). Once a copyright owner discovers a probable infringer, it must prepare and submit a notification, just as it would for a typical takedown request.[99] The copyright owner may then request from the clerk of the issuing court a subpoena for the subscriber information of the allegedly infringing user.[100] This request must be filed with the following:

> (A) a copy of a notification described in subsection (c)(3)(A) [the takedown notification];
>
> (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.[101]

Upon receiving this request, the clerk of the court *must* "expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider" if it properly satisfies these three requirements.[102] At no point in the process does the clerk exercise any independent discretion in evaluating the subpoena nor does a judge ever become involved at this stage.[103] Once the clerk issues the subpoena, the copyright owner serves it on the appropriate designated agent of the service provider.[104] Upon receipt of the subpoena, "the

---

[99] *Id.* *See also supra* note 65 and accompanying text (quoting the requirements for the takedown notification).

[100] § 512(h)(1).

[101] § 512(h)(2)(A)-(C).

[102] § 512(h)(4) ("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.").

[103] *Verizon II*, 257 F. Supp. 2d at 250. *See also* Fed. R. Civ. P. 45(a)(3) (describing similar procedures for the issuance of a federal subpoena).

[104] § 512(c)(2). Although subsection (c)(2) does not expressly provide that the subpoena must be served on the designated agent, it is a logical conclusion because subsection (c)(2) requires the takedown notification to be

service provider shall expeditiously disclose to 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 [takedown] notification."[105]

Together with the structure of section 512, this language makes it very clear that there is no formal statutory process in place for contesting the appropriateness of the subpoena comparable to that provided for challenging a takedown notification.[106] Such an appeal process would seem to be even more necessary with respect to a subpoena because the release of a subscriber's identity cannot be undone. Erroneously removed Internet content can be replaced, but identity information cannot be unlearned. Thus, it is important that such information not be released erroneously in the first place. Additionally, section 512(h) does not require service providers to give notice to subscribers whose information has been subpoenaed under the DMCA, which only compounds the problem and makes the inappropriate or mistaken release of identity information that much more likely.[107]

Once a service provider receives a section 512(h) subpoena requesting the identification information of one of its subscribers, it basically has two options: respond to the subpoena with the appropriate information or challenge the subpoena with a motion to quash. As mentioned above, until the RIAA announced its new strategy to pursue actions directly against individual

---

delivered to the designated agent and subsection (h)(5) requires the subpoena to be served on the service provider either accompanying or subsequent to the delivery of the notification. *Id.*; § 512(h)(5).

[105] § 512(h)(5).

[106] Section 512(h) does not contain a procedure similar to that found in subsection (g) for challenging the removal of allegedly infringing material.

[107] Davidson, *supra* note 27. Note, however, that nothing in section 512 expressly prevents a service provider from giving notice to its subscribers if their information has been subpoenaed.

infringers, service providers always chose the first option.[108] Realizing that a dangerous new trend was in the offing, Verizon Internet Services created quite a stir in the legal community when it became one of the first ISPs to bring a significant challenge to a subpoena issued under section 512(h).[109] Several other service providers, including two major universities, which act as service providers to their faculty and students, have followed Verizon's lead in filing motions to quash subpoenas served on them by the RIAA.[110] These cases have raised various interpretational issues and perceived problems—both constitutional and statutory—with respect to the DMCA provision. Before Part IV discusses these issues, challenges, and the cases in which they have been raised, it is crucial to understand why this conflict between the service providers and copyright holders over section 512 arose in the first place.

D. How was the DMCA Supposed to Work?

Clearly, there is serious confusion concerning just how the subpoena provision was intended to operate within the context of section 512. The existence of this confusion is somewhat surprising considering that the two adversaries in this conflict, the music recording industry and the ISPs, were significantly responsible for the enacted version of section 512.[111] These two sides worked together with legislators to craft a set of laws that would allow for the enforcement of copyrights and protect service providers from liability for their customers' violations. There would seem to be no rational explanation for conflict or confusion in a

---

[108] *See supra* note 37 and accompanying text.

[109] *Verizon I*, 240 F. Supp. 2d at 26 (noting that this case, which involved the interpretation of the DMCA subpoena provision, presented an issue of first impression).

[110] *See supra* note 38 and accompanying text.

[111] S. REP. NO. 105-190, at 9. Indeed, representatives of Verizon and the RIAA were personally involved in the negotiation of section 512. Declan McCullagh, *Verizon's Copyright Campaign*, CNET News.com (Aug. 27, 2002) (interview with Sarah Deutsch, Vice President & Associate General Counsel, Verizon Internet Services, Inc.), *at* http://news.com/2008-1082-955417.html (last visited Feb. 17, 2004).

compromise to which these parties willingly agreed in the first place. Granted, various factors have arisen that neither side could have anticipated when negotiating the compromise that became Section 512 of the DMCA,[112] but could recent technological developments by themselves have stirred up the turmoil that surrounds the DMCA subpoena provision today?

The answer to this question seems to lie in the additional fact that none of these issues arose until the RIAA announced its new strategy of suing individual infringers on a national scale.[113] No longer are the copyright holders merely issuing subpoenas in conjunction with takedown notices for infringing material actually residing on service providers' systems or networks. Copyright holders are now issuing subpoenas for the identity of subscribers merely transmitting infringing material via their service providers' networks, activity that is covered under subsection 512(a).[114] This would not have been possible, at least not on a large scale, before the development of bots and P2P networks. Before these two recent technological developments, copyright owners really had no method or tool for discovering infringing material unless it was physically posted on the Internet, which would generally require that the material reside on the systems or networks of the infringer's ISP.[115] In these situations, copyright owners would simply issue takedown notices to the appropriate service providers pursuant to section 512(c) and occasionally serve subpoenas in the rarer event that the notices were ignored or the

[112] *Verizon I*, 240 F. Supp. 2d at 23 (noting that the development of both P2P software and bots had not yet occurred and were not anticipated at the time of the DMCA's discussion and enactment). Without a doubt, these two factors played a significant role in creating the immense conflict currently raging between service providers and copyright owners, but they were likely more in the nature of catalysts than causes.

[113] *See supra* notes 37-38 and accompanying text.

[114] McCullagh, *supra* note 111.

[115] Tools able to search through material as it is sent and received by a service provider, known as "packet sniffers," remain cutting-edge technology and are not readily available to the public.

copyright holder felt a lawsuit was warranted by the seriousness of the infringement.[116] It appears that at least the service providers expected that this was how section 512, and especially the subpoena provision, was intended and would continue to operate. This perspective is supported by Verizon's repeated arguments that section 512 was primarily intended as a notice and takedown provision and that the subpoena authority is restricted to situations involving infringing materials actually residing on service providers' systems or networks.[117]

The introduction of P2P networks and search bots changed the entire context of section 512 and how it could be used to enforce copyrights. In addition to creating centralized lists of digital files available for sharing, P2P networks also essentially created readily available, searchable lists of infringement and infringers. The employment of search bots and rangers has made the task of combing these networks for infringement extremely fast and efficient.[118] These two developments have allowed copyright owners to begin seeking out infringing activity covered under the subsection (a) safe harbor provision—involving the transmission of infringing material over the systems and networks of service providers—in addition to infringement covered under subsection (c)—involving the storage of infringing material on the service provider's systems or networks. Of course, infringing material was transmitted over service providers' networks long before P2P networks appeared on the digital transfer scene,[119] but copyright owners really had no method of tracking such traffic. Ironically, the development of

[116] Wikipedia, *Online Copyright Infringement Liability Limitation Act*, *at* http://en.wikipedia.org/wiki/OCILLA (last visited Feb. 17, 2004).

[117] *See e.g.*, Manjoo, *supra* note 37 (quoting Sarah Deutsch, associate general counsel for Verizon: "I was one of the 10 industry representatives who was there to draw up this law…and it was clearly our interpretation that the content would have to be on our network. We agreed to a process called 'notice and takedown' for material that was on the network.").

[118] *See* Skelton, *supra* note 30, at 5.

[119] E-mail, instant messaging, and ftping are still commonly used methods for transferring files directly between users.

P2P networks, which enabled users to more easily engage in copyright infringement, also enabled copyright owners to more easily discover such infringement.

The development of P2P networks and search bots has thus wrought several major changes in the manner in which copyrights are enforced online. Most importantly, copyright owners are now taking action against users merely transmitting infringing files across their service providers' networks as well as those users actually uploading infringing files onto their service providers' systems for hosting purposes. Once copyright owners realized that the first type of infringement far outweighed the second type, it was only a matter of time before they responded accordingly by issuing section 512(h) subpoenas.[120]

Due to the fact that no one expected that subsection 512(a) would ever serve as a basis for exercising the subpoena authority like subsection 512(c),[121] a fierce debate has risen as to whether copyright holders may issue a subpoena for the identity of a subscriber who merely transfers infringing materials across a provider's network, but does not store such materials on the provider's servers. Copyright owners argue that the power to issue subpoenas to service providers protected under subsection (a) has always existed in section 512, regardless of whether such use was foreseen. They reason that, by including in section 512 each of the four safe harbor subsections that limit the liability of service providers, Congress intended to protect from secondary liability the gamut of service provider functions that could be used by subscribers to engage in infringement.[122] At the same time, Congress also intended to give copyright owners recourse, through the help of service providers, against infringers in each of those four

[120] *Verizon I*, 240 F. Supp. 2d at 35 (noting that P2P networks provide the largest opportunity for online copyright infringement).

[121] *Verizon Appeal*, 351 F.3d at 1238.

[122] *Verizon I*, 240 F. Supp. 2d at 27.

situations.[123] The fact that copyright owners did not have until recently the capabilities necessary to take advantage of that recourse in one or more of those prescribed situations does not mean that the recourse never existed.[124]

On the other hand, ISPs contend that the language of section 512 precludes the issuance of a subpoena to a service provider merely acting as a conduit for the transmission of infringing material across its networks.[125] Pursuant to the subpoena provision, the proposed subpoena offered to the Clerk of the Court must contain a copy of a takedown notification.[126] Such a notification must identify the material "to be removed or access to which is to be disabled" by the service provider.[127] The service providers maintain that satisfaction of these requirements is impossible in situations falling under subsection (a).[128] Their argument is essentially that where a subscriber is merely transmitting infringing material over their networks, the ISP does not possess the ability to remove or disable access to such material, which is not on its servers.[129] Thus, there can be no proper takedown notification under subsection (a) and, hence, no subpoena based on that subsection.[130] Significantly, the fact that subsection (a) never even refers to the

[123] *Id.* at 34.

[124] Part IV.A.1, *infra*, will discuss how the structure and legislative history may support this conclusion that the DMCA subpoena power was intended to apply to infringement in the context of all four types of service provider functions: transmitting, system caching, hosting, and linking (not necessarily hosting alone, as argued by Verizon).

[125] *Verizon Appeal*, 351 F.3d at 1233.

[126] 17 U.S.C. § 512(h)(2)(A) (2000).

[127] § 512(c)(3)(A)(iii).

[128] *Verizon Appeal*, 351 F.3d at 1234-35.

[129] *Id.*

[130] *Id.* at 1235.

takedown notification, while subsections (b) through (d) do, supports the service providers' argument.[131]

Neither party could have anticipated that the subpoena power would be used in the manner in which it is currently being employed, and now the service providers are fighting a monster that they themselves helped to create. Now that the issue of how section 512 was intended to work has been addressed, a vital question still remains: how *should* section 512 work? An answer to this question may not provide a resolution for all the issues that have been raised against the DMCA subpoena provision, but it may help the legislature to understand the need for changes in the provision and what those changes should be. Beginning the journey toward this goal, Part IV will discuss the various issues that have been raised with respect to the DMCA subpoena provision, highlighting the arguments of both the service providers and copyright owners in the recent cases, as well as the opinions of the courts.

IV. ISSUES REGARDING THE CURRENTLY ENACTED DMCA SUBPOENA PROVISION

The cases in which service providers have challenged subpoenas issued pursuant to section 512(h) have involved issues falling into three primary categories: (1) statutory construction issues, (2) constitutional issues, and (3) policy issues concerning the provision's potential for abuse.[132] Initially, the major service providers were hesitant to raise constitutional issues with respect to the subpoena provision because they had played such an integral role in the original drafting process of Title II of the DMCA.[133] Instead, the service providers focused on

[131] *Id.* at 1234.

[132] *See generally Verizon Appeal*, 351 F.3d 1229 (D.C. Cir. 2003).

[133] *See* McCullagh,*supra* note 111.

statutory construction and interpretation issues, leaving the constitutional issues to be argued by privacy and consumer rights advocates, such as the Electronic Frontier Foundation and the Center for Democracy & Technology, in their amicus curiae briefs.[134] The service providers quickly realized, however, that they would need all the legal ammunition they could acquire to levy a successful challenge against the subpoena provision and they began objecting to the subpoenas on several constitutional grounds as well.[135] Each of these challenges to the DMCA subpoena power will be discussed in turn.

A. Statutory Construction Issues

1. To What Types of ISPs does the Subpoena Provision Apply?

In the first Verizon case, which has been referred to in this Article as *Verizon I*, the service provider primarily argued that the section 512(h) subpoena provision did not apply to it because it was serving only as a conduit for the infringing activity of the subscriber at issue.[136] Verizon contended that it merely provided Internet access to the allegedly infringing subscriber and that the subpoena provision was only intended to apply to service providers actually hosting the allegedly infringing material on their systems or networks.[137] Because its activities fell within the scope of the safe harbor provision in subsection (a) for service providers acting as a conduit for the transmission of infringing material, not within the scope of the safe harbor provision in subsection (c) for service providers hosting infringing material on their systems or

[134] *See e.g.*, *Verizon I*, 240 F. Supp. 2d at 41-42 (noting that Verizon did not assert that the section 512(h) subpoena power is unconstitutional; those issues were only raised by the amici curiae supporting Verizon).

[135] *See e.g.*, *Verizon II*, 257 F. Supp. 2d at 246-47 (noting that in Verizon I, the service provider only challenged the RIAA's subpoenas on the basis of statutory construction, but that in the present case, Verizon also challenged the constitutionality of the subpoena provision).

[136] *Verizon I*, 240 F. Supp. 2d at 29.

[137] *Id.* (discussing Verizon's argument that its activities fell within the safe harbor provision of subsection (a) and that that the subpoena provision only applies to service providers whose conduct falls within the activity described in subsection (c)).

networks, Verizon argued that the takedown notification provision, which is found within subsection (c)(3)(A), did not apply to it and consequently neither did the subpoena provision.[138]

On the other hand, the RIAA argued that the subpoena provision and subsection (c)(3)(A), detailing the requirements for the notification provision, are freestanding provisions, which are referenced in several other areas outside of subsection (c).[139] Thus, according to the RIAA, the notification and subpoena provisions apply to service providers engaging in each of the four types of activities granted safe harbor under the DMCA, not merely to service providers that are actually hosting infringing material on their systems or networks.[140] Based on this interpretation, the subpoena was valid no matter which safe harbor Verizon fell under.[141]

Finding none of Verizon's arguments entirely persuasive, the District Court for the District of Columbia adopted the RIAA's interpretation of section 512.[142] The court supported its decision with a convincing array of reasons. First, the court found that "[t]he statutory text of the DMCA provides clear guidance for construing the subpoena authority of subsection (h) to apply to *all* service providers under the act."[143] The term "service provider" is clearly referenced throughout the subpoena provision.[144] Significantly, section 512 provides two distinct definitions of service provider in a freestanding definition section: "a narrow definition as the term is used solely within subsection (a), and a broader definition governing all other

---

[138] *Id.*

[139] Motion to Enforce July 24, 2002 Subpoena Issued by this Court to Verizon Internet Services, Inc. and Memorandum in Support Thereof at 14, *Verizon I*, 240 F. Supp. 2d 24 (D.D.C. 2003).

[140] *Id.* at 15.

[141] *Verizon I*, 240 F. Supp. 2d at 29, n.3.

[142] *Id.* at 39.

[143] *Id.* at 30 (emphasis added).

[144] *Id.* (citing specific examples).

subsections, which specifically includes a "service provider" under subsection (a) as well."[145] Based on this express two-part definition of "service provider" found in subsection (k), the court found it clear that the broader, all-encompassing definition applies to the term as it is used in the subsection (h) subpoena provision.[146] Thus, it held that the subpoena provision applies to all service providers, including those engaged in activities described in each of the safe harbor provisions.[147]

Second, the court held that Verizon's interpretation was strained and conflicted with the overall structure of section 512 because the subsection (c)(3)(A) notification provision is referenced in several other places in section 512 outside of the subsection (c) safe harbor provision.[148] Thus, the notification provision must necessarily apply outside of the context of subsection (c) and its safe harbor for ISPs hosting infringing material on their systems and networks.[149] In addition, the section 512(h) subpoena provision is not limited or restricted in any

[145] *Id.* (citing § 512(k)). Section 512(k) states:

> (k) Definitions.
>
> (1) Service provider.
>
> (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
>
> (B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A).

[146] *Id.* at 31 (noting that the subsection (c)(3)(A) notification provision is referenced in both the subsection (b) and (d) safe harbor provisions for system caching of and linking to infringing material).

[147] *Id.*

[148] *Id.* at 32.

[149] *Id.*

fashion to service providers covered under subsection (c).[150] The subpoena provision is located in a freestanding subsection and is in no way solely tied to service providers falling within the scope of subsection (c).[151]

Finally, the court noted that Verizon's interpretation conflicted with Congressional intent with respect to section 512.[152] If Verizon's interpretation were adopted, "the statute would fail significantly to address many contexts in which a copyright owner needs to utilize the subpoena process in order to discern the identity of an apparent copyright infringer."[153] Verizon's interpretation would prevent a copyright owner from having any recourse against a subscriber who merely used his or her Internet service for the transmission of infringing files. Thus, Verizon's interpretation "would create a huge loophole in Congress's effort to prevent copyright infringement on the Internet," through which infringing users of P2P networks would be able to escape liability.[154] Clearly, Congress could not have intended such an effect.

Supporting its holding textually, structurally, and with legislative intent, the *Verizon I* court convincingly laid Verizon's interpretation of section 512 to rest. On appeal, however, the DC Circuit reversed the trial court's decision and resurrected Verizon's position based on a textual analysis.[155] The Court of Appeals analyzed section 512 in the same manner as the district

[150] *Id.* at 33 (noting that if Congress had intended for the subpoena provision to merely apply to subsection (c) situations, it would have placed the provision within subsection (c), named the provision to reflect its application to a narrow subset of service providers, or taken other similar explicit measures).

[151] *Id.*

[152] *Id.* at .

[153] *Id.* at 34.

[154] *Id.* at 35.

[155] *Verizon Appeal*, 351 F.3d at 1231.

court, looking to the text and the structure of the statute before turning to the legislative intent and purpose, but focused on different elements of the statute to arrive at the opposite conclusion.

Beginning its opinion with an examination of the text of section 512, the court agreed with Verizon's argument that the subpoena provision does not apply to service providers acting merely as a conduit for P2P communications.[156] The court reasoned that the statute expressly provides that the issuance of a subpoena under section 512(h) requires a takedown notification,[157] which must identify the allegedly infringing material "that is to be removed or access to which is to be disabled."[158] The takedown notification requirement is a condition precedent to the issuance of a subpoena under section 512(h).[159] Because Verizon was merely acting as a conduit for the transmission of infringing material on P2P networks and was not storing the infringing material on its server, the RIAA could not identify material to be removed or access to which is to be disabled.[160] A service provider merely acting as a conduit for the transmission of infringing material can neither "remove" nor "disable access to" the material because it is not stored on the provider's servers.[161] Since it does not control the content on its subscribers' computers, it cannot actually remove or disable access to the infringing material.[162] Since this crucial requirement for the takedown notification cannot be satisfied where the service

[156] *Id.* at 1233.

[157] *Id.* at 1234 (citing § 512(h)(2)(A)).

[158] *Id.* at 1235 (quoting § 512(c)(3)(A)(iii)).

[159] *Id.* (quoting § 512(h)(4), "'If the notification filed satisfies the provisions of § 512(c)(3)(a)' and the other content requirements of § 512(h)(2) are met, then 'the clerk shall expeditiously issue and sign the proposed subpoena…for delivery' to the ISP.").

[160] *Id.*

[161] *Verizon Appeal*, 351 F.3d at 1235.

[162] *Id.*

provider is merely acting as a conduit, the takedown notification requirement for obtaining a subpoena cannot be met, and thus no subpoena may be issued.[163]

The RIAA contended that a service provider can disable access to infringing material "by terminating the offending subscriber's Internet account."[164] The court rejected this argument based on the fact that Congress expressly treated disabling a subscriber's access to infringing material and disabling access to the Internet as two distinct remedies.[165] The court compared section 512(j)(1)(A)(i), which authorizes an injunction restraining an ISP "from providing access to infringing material," with section 521(j)(1)(A)(ii), which authorizes an injunction restraining an ISP "from providing access to a subscriber or account holder…who is engaging in fringing activity…by terminating the accounts of the subscriber or account holder."[166] Noting that "where different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings," the court concluded that the provision of these two distinct remedies establishes 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."[167]

The Court of Appeals further bolstered its opinion with an analysis of the structure of section 512.[168] Verizon noted that section 512(h), the subpoena provision, specifically references the takedown notification provision, which is found in subsection (c), but does not

---

[163] *Id.* at 1234-35.

[164] *Id.* at 1235.

[165] *Id.*

[166] *Id.*

[167] *Verizon Appeal*, 351 F.3d at 1235.

[168] *Id.* at 1236-37.

explicitly reference subsections (a), (b), or (d).[169] Verizon thus argued that the subpoena provision only applies to situations governed by subsection (c), where the service provider hosts the infringing material on its servers.[170] Despite rejecting Verizon's overly broad contention that the subpoena provision *only* applies to section 512(c) cases, the court agreed with Verizon's narrower conclusion that it does not apply to section 512(a).[171] The court pointed out that subsections (b) and (d), which govern a service provider's temporary storage of infringing material on its systems and a service provider's hosting of a tool linking users to infringing material, respectively, both cross-reference the takedown notification provision upon which the subpoena provision relies.[172] Thus, the court concluded that the subpoena provision also applies to subsections (b) and (d).[173] This rationale is logical because, as the court noted, all three subsections involve a service provider's storage of infringing material on its servers in some capacity.[174] Subsection (a), however, does not involve such storage, but rather the transmission of infringing material. As described above, because the service provider does not have the ability to remove or disable access to infringing material not stored on its systems or network, it makes sense that subsection (a) does not reference the takedown provision and that the subpoena provision does not apply to subsection (a).[175]

---

[169] *Id.* at 1236.

[170] *Id.*

[171] *Id.* at 1237.

[172] *Id.*

[173] Verizon Appeal, 351 F.3d at 1237.

[174] *Id.*

[175] *Id.*

Looking to the purpose and legislative intent behind section 512, the court did note that it was unfortunate that Congress was not able to anticipate the creation of P2P technology and accordingly draft legislation that would fully protect copyrights from digital infringement.[176] The court held that despite the fact that Congress likely did not intend to leave such a broad loophole in the copyright enforcement law, it is not the place of the courts to "rewrite the DMCA in order to make it fit a new and unforeseen Internet architecture, no matter how damaging that development has been to the music industry…"[177] The court concluded that this problem must be addressed by Congress because only "'Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.'"[178]

Although the Court of Appeal's decision seems somewhat unfair from a policy perspective, it was the right one in terms of balancing long-term interests. The court recognized the harm that illegal P2P file sharing has done to the entertainment industry, but correctly concluded that it did not have the resources to properly take into account the many competing interests and the high stakes involved.[179] This decision properly placed the weight of resolving the many issues that have arisen with respect to the DMCA subpoena provision squarely on the shoulders of Congress, where it belongs. As of the time that this case was decided, Congress had already begun to address the task of updating digital copyright protection legislation to deal with P2P technology.[180] Unfortunately, the Court of Appeals did not address the constitutional

[176] *Id.* at 1238.

[177] *Id.*

[178] *Id.*

[179] Verizon Appeal, 351 F.3d at 1238..

[180] *Id.* at 1238-39.

challenges that Verizon brought against the subpoena provision, which were rejected by the district court.[181] Analyses of these issues would have been well within the court's province and would have provided Congress with valuable guidance in restructuring section 512.

2. Does Section 512(h) trump Rule 45 of the Federal Rules of Civil Procedure?

Another significant constructional issue relates to the interpretation of the DMCA in the context of the Federal Rules of Civil Procedure. The section 512(h) subpoena provision grants copyright owners enhanced subpoena authority that is significantly greater than that offered by Rule 45.[182] One of the major debates regarding the confluence of these two subpoena provisions is whether the DMCA subpoena power trumps the geographic limitation requirements set out in Rule 45.[183] The Massachusetts Institute of Technology (MIT) first raised this issue in court after it received a subpoena from the RIAA demanding the subscriber information of an allegedly infringing student.[184] Before analyzing this case, it is necessary to briefly describe the provisions relating to service and delivery of subpoenas under both Rule 45 and section 512.

Section 512(h) provides that "[a] copyright owner…may request the clerk of *any* United States district court to issue a subpoena to a service provider for identification of an alleged infringer…"[185] It further mandates that "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

---

[181] *Id.* at 1231.

[182] *See* McCullagh, *supra* note 111 (referring to the DMCA subpoena provision as "turbocharged").

[183] *District of Columbia Court Lacks Authority to Issue DMCA Subpoenas to Boston Schools*, 66 ELECTRONIC COM. & L. REP. No. 1634, at 459 (Aug. 15, 2003).

[184] In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MC-10209-JLT (Aug. 7, 2003).

[185] 17 U.S.C. § 512(h)(1) (2000) (emphasis added).

the issuance, service, and enforcement of a subpoena duces tecum."[186] Rule 45 is the relevant provision pertaining to subpoenas duces tecum in the Federal Rules of Civil Procedure. It states that "a subpoena for production or inspection shall *issue* from the court for the district in which the production or inspection is to be made."[187] In addition, a subpoena may be *served* at any place within the district of the issuing court *or* at any place outside the district that is within 100 miles of the location where the subpoena is served.[188] Rule 45, however, also states that "when a statute of the United States provides therefor, the court upon proper application and cause shown may authorize the service of a subpoena at any other place."[189] Basically, Rule 45 allows federal law to mandate nationwide service of process when appropriate.

In the case of *In re Subpoena to the Massachusetts Institute of Technology*,[190] MIT initially noted in its memorandum in support of its motion to quash that section 512(h) requires that "'the procedure for issuance and delivery' of any subpoena issued pursuant to the DMCA '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.'"[191] Accordingly, MIT argued that the subpoena served by the RIAA violated the

---

[186] § 512(h)(6).

[187] FED. R. CIV. P. 45(a)(2) (emphasis added).

[188] *Id.* 45(b)(2).

[189] *Id.*

[190] Note that the RIAA obtained the subpoena from the United States district Court for the District of Columbia and filed its motion to enforce the subpoena with that court. In re Subpoena to Mass. Inst. of Tech., No. 1:03-MS-00265 (D.D.C. motion to enforce filed Aug. 1, 2003). MIT, however, moved to quash the subpoena in the District Court for the District of Massachusetts. In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MC-10209-JLT (motion to quash filed July 21, 2003). Although complicating the procedural history, this twist does not alter the substantive issues in the case.

[191] Memorandum of the Massachusetts Institute of Technology in Support of its Motion to Quash Subpoenas and for a Protective Order at 4, In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MC-10209-JLT (Aug. 7, 2003) [hereinafter MIT Memorandum].

geographic limitations imposed by Rule 45 because they were issued from the United States District Court for the District of Columbia and served on MIT in Massachusetts to produce documents in Washington, D.C.[192] According to MIT, the RIAA's subpoena did not comport with the restrictions of Rule 45 for either the issuance or the service of subpoenas duces tecum. First, Rule 45(a)(2) provides that a subpoena for the production of documents must issue from the court for the district in which the production is to be made. [193] In this case, the subpoena issued from Washington, D.C., but the production was to be made from Massachusetts. Second, the RIAA's subpoena violated the rule governing service, which provides that subpoenas must be served within the district of the issuing court.[194] Although Rule 45(b)(2) also provides that subpoenas may be served outside the district from which they issue, this option only applies if the place of service is "within 100 miles of the place of the…production specified in the subpoena."[195] Because Massachusetts, the place of service, is clearly more than 100 miles from Washington, D.C, the place of production, the option does not apply. MIT noted that Rules 45(a)(2) and (b)(2) together "require that a subpoena duces tecum be issued from a convenient United States District Court, so that a third-party like MIT may seek judicial assistance without the burden of traveling to a distant district."[196] MIT contended that the RIAA's subpoena should

[192] *Id.* at 5.

[193] *Id.* (citing FED. R. CIV. P. 45(a)(2)).

[194] FED. R. CIV. P. 45(b)(2).

[195] MIT Memorandum at 5 (quoting FED. R. CIV. P. 45(b)(2)).

[196] *Id.* at 5-6 (admitting that the production of records in response to the RIAA's subpoena would not be inconvenient or burdensome in and of itself, but asserting that having to litigate the validity of the subpoena in a distant forum would be inconvenient and burdensome).

be quashed because it violated both the rules governing the issuance and service of subpoenas duces tecum and the policies underlying those rules.[197]

In its motion to enforce the subpoena, the RIAA responded with several counterarguments to these issues that MIT raised in its motion to quash. First, the RIAA contended that subpoenas issued pursuant to the DMCA are not subject to the territorial limitations imposed on subpoenas issued pursuant to Rule 45 because "Congress intended the DMCA subpoena process to be streamlined and expeditious to fulfill its functions."[198] The DMCA subpoenas, the RIAA argued, "are not broad discovery mechanisms" like Rule 45 subpoenas, but rather "are targeted to ensure that a discrete amount of information is made available for the limited purpose of enabling a copyright owner to pursue its rights."[199] Based on clear Congressional intent, DMCA subpoenas must enable copyright owners to enforce their rights quickly and efficiently "notwithstanding any other provision of law."[200] According to the RIAA, MIT's interpretation conflicts with this intent by slowing and burdening the DMCA subpoena process. Essentially, MIT's interpretation would force copyright owners "to have counsel in every one of the 94 judicial districts, ready at a moment's notice to serve subpoenas."[201]

The RIAA claimed that this conclusion is also supported by the language of section 512(h)(6), which states that "*unless otherwise provided by this section*…, the procedure for

[197] *Id.* at 6-7.

[198] Motion to Enforce Subpoena to MIT at 10

[199] *Id.*

[200] *Id.* at 12-13 (quoting § 512(h)(5)).

[201] *Id.* at 13. The RIAA noted that "[i]n tracking down a single infringer, a copyright owner may have to obtain multiple subpoenas to multiple ISPs. Forcing the copyright owner to go to multiple courts to identify one infringer is a burden that would seriously frustrate the goals of the DMCA." *Id.* at 13 n.3. While this unlikely scenario is somewhat of an exaggeration, the underlying argument is not without merit.

issuance and delivery of the subpoena…shall be governed to the greatest extent practicable0" by Rule 45.[202] This language, according to the RIAA, makes it clear that although the procedures of Rule 45 generally apply to subpoenas issued pursuant to the DMCA, Rule 45 is inapplicable "whenever it would conflict with section 512(h) or when application of Rule 45 would not be practicable, given the goals that section 512(h) advances."[203] The application of the geographical restrictions in this case would thwart the goals of section 512(h) and the purpose of the DMCA.[204]

Second, the RIAA contended that even if traditional service under Rule 45 would normally be required for DMCA subpoenas, the DMCA authorizes nationwide service of process. In cases involving the enforcement of federal law, Congress has the power to authorize, either expressly or impliedly, nationwide service of process,[205] and Section 512(h)(1) of the DMCA authorizes the issuance of subpoenas by the "clerk of *any* United States district court."[206] The RIAA based its contention on various cases involving subpoena provisions within other federal statutes, such as the Federal Trade Commission Act (FTC Act) and the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA).[207] The RIAA argued that these cases suggest that the determination of whether a statute authorizes nationwide service

[202] *Id.* at 13-14; § 512(h)(6) (emphasis added).

[203] Motion to Enforce Subpoena to MIT, at 13-14.

[204] *Id.* at 14.

[205] *Id.* (citing Mariash v. Morrill, 496 F.2d 1138, 1143 n.6 (2d Cir. 1974); United States v. Congress Constr. Co., 222 U.S. 199 (1911); Robertson v. R.R. Labor bd., 268 U.S. 619, 622 (1925); First Nat'l Bank of Canton v. Williams, 252 U.S. 504, 509-510 (1920); United States v. Bliss, 108 F.R.D. 127, 135 (E.D. Mo. 1985)).

[206] § 512(h)(1) (emphasis added).

[207] Motion to Enforce Subpoena to MIT at 14-16.

depends on the policy goals of the particular statute and whether nationwide service is necessary to effectuate those goals.[208]

With respect to the RIAA's second argument, MIT countered that the phrase "any United States district court" merely signifies "that a copyright holder need not go to any particular court to issue a DMCA subpoena, but may instead have it issued from any district in the federal court system that has authority to issue such a subpoena. Citing to *Robertston v. Railroad Labor Board*, MIT noted that the U.S. Supreme Court expressly rejected the RIAA's contention when it held that the phrase, "any District Court of the United States," merely referred to "a court that has jurisdiction under otherwise applicable rules to issue the subpoena."[209] MIT also attempted to distinguish several of the cases cited by the RIAA based on the fact that they involved statutes that much more explicitly authorized nationwide service of process.[210] Quoting *Federal Deposit Insurance Corporation v. Abrams*,[211] MIT concluded, "Congress knows how to authorize nationwide service of process when it wants to provide for it. That Congress failed to do so…argues forcefully that such an authorization was not its intention."[212]

The issue of whether the DMCA subpoena power trumps the procedural requirements mandated by Rule 45 remains essentially unresolved. While the Massachusetts district court granted MIT's motion to quash, it did so in a single sentence opinion, which did little to shed

---

[208] *Id.* at 15.

[209] MIT Memorandum at 8.

[210] *Id.* at 8-9. The FTC Act authorizes subpoenas to be enforced by "[a]ny of the district courts of the United States *within the jurisdiction of which such inquiry is carried on*." 15 U.S.C. § 49 (2000) (emphasis added).

[211] 893 F. Supp. 4 (D. Mass. 1995).

[212] MIT Memorandum at 9 (quoting *Abrams*, 893 F. Supp. at 5).

light on how the courts will approach this issue in the future.[213] Instead of challenging the Massachusetts district court's order, it appears that the RIAA will simply refile for a second subpoena in that court,[214] which will delay a more substantial resolution of this issue until it is raised again.

It is difficult to predict which side the courts will favor on this issue. Comparing the arguments of the RIAA and MIT in this case, each has its strengths, but MIT's interpretation appears to be the more sound of the two. A purely textual reading seems to support MIT's position that a subpoena issued pursuant to the DMCA must comply with the geographical limitations of Rule 45, especially in light of the Supreme Court's decision in *Robertson*, which held that the phrase relied on by the RIAA does not by itself authorize nationwide service.[215] In addition, section 512(h)(6) clearly states that the procedure for *issuance and delivery* of the DMCA subpoena is to be governed by the provisions of Rule 45, unless otherwise provided by section 512. Outside of subsection 512(h), the only provision discussing procedure for issuance or delivery may be found in subsection (c)(2), which establishes that takedown notifications must be delivered to the service provider's designated agent.[216] Nothing in the language of section 512 expressly conflicts with the application of Rule 45. Textually, there is little support for the RIAA's interpretation that the geographical limitations of Rule 45 do not apply to DMCA subpoenas.

---

[213] In re Subpoena to the Mass. Inst. of Tech., No. 1:03-MC-10209-JLT (Aug. 7, 2003) ("Because Fed. R. Civ. P. 45(a)(2) and (b)(2) do not permit a subpoena for production issued in Washington, D.C. to be validly served in Massachusetts, Plaintiff's Motion to Quash Subpoena and for Protective Order [#1] is ALLOWED.").

[214] Keith J. Winstein, *RIAA Will Issue Second Subpoena for Identity of Music Distributor*, The Tech (Aug. 22, 2003), *at* http://www-tech.mit.edu/V123/N31/31riaa.31n.html (last visited Feb. 17, 2004). Theoretically, the District Court for the District of Columbia could order MIT to comply with the subpoena, thereby creating a conflict; however, this is unlikely given that the RIAA has agreed to file in the Massachusetts court.

[215] *Robertson*, 268 U.S. at 627.

[216] 17 U.S.C. § 512(c)(2) (2000).

From a policy perspective, however, the RIAA raises a legitimate point that one of the primary purposes of section 512 is to enable the enforcement of copyrights in an expedient manner.[217] But would the imposition of the geographical limitations of Rule 45 significantly obstruct this goal as the RIAA contends?[218] Although the RIAA was guilty of exaggeration when it suggested that such restrictions would require copyright owners "to have counsel in every one of the 94 judicial districts, ready at a moment's notice to serve subpoenas," imposing the geographical limitations of Rule 45 would indeed place a large burden on copyright owners.[219] Once the conflict concerning the interpretation of section 512 has been substantially resolved, the number of valid and accurate subpoenas will almost certainly be far greater than the number of erroneous subpoenas that must be challenged. This would suggest, in the interest of efficiency, that the RIAA's interpretation be adopted. Rather than forcing copyright owners to obtain subpoenas from different jurisdictions each time a new service provider is involved, efficiency would be maximized by forcing the service provider to challenge the subpoena in the issuing court in the much rarer event that a subpoena is invalidly or mistakenly issued.

For example, copyright owner X issues DMCA subpoenas to three different service providers in districts A, B, and C. Only the subpoena to the service provider in district C is mistakenly issued. If the geographic limitations of Rule 45 were imposed, then X would have to retain counsel in each of those three jurisdictions to obtain and serve the three subpoenas, which would be a substantial burden. The service provider in C, however, would not be significantly burdened in challenging the subpoena it received in the district C court. Essentially, in this

[217] Motion to Enforce Subpoena to MIT at 11-12.

[218] *Id.* at 13.

[219] *Id.*

situation, the three subpoenas would result in a total of three substantial burdens, all falling on the shoulders of the copyright owner, X.

On the other hand, if the geographic limitations of Rule 45 were not applied to DMCA subpoenas, then X would merely serve each of the three service providers with subpoenas issued from the court in X's district. Because the subpoenas issued to the service providers in districts A and B are accurate, there would be no substantial burden as a result of their compliance.[220] If the service provider in district C were unable to convince X that the subpoena issued to it was invalid or mistaken, then the service provider would have to retain counsel in X's district to challenge the subpoena. Thus, under the same circumstances, the three subpoenas would only result in at most one substantial burden, this time falling on the shoulders of the service provider in district C.

This rather lengthy example demonstrates that the RIAA's interpretation would likely be more efficient in the long term when all the parties are taken into account. This is especially true considering that the ratio of proper to erroneous DMCA subpoenas is likely greater than 2 to 1. Excluding the geographic limitations of Rule 45 would also allow for more expeditious enforcement of copyrights, thereby affording more protection for copyright owners.

It is not clear from the text of the DMCA or from its legislative history whether Congress intended such a result.[221] Due to the conflicting case law raised by the two sides, this issue is much better resolved by Congress. Congress could easily amend section 512(h)(6) to explicitly incorporate or exclude the geographical limitations of Rule 45, as it has done for other federal

[220] MIT Memorandum at 6 (admitting that responding to DMCA subpoenas is not itself inconvenient or burdensome).

[221] As noted in the preceding discussion, the text seems to imply that DMCA subpoenas are subject to the geographic limitations of Rule 45, but the legislative history seems to suggest that the imposition of such limitations would defeat the overarching goal of expeditious copyright enforcement.

statutes.[222] While excluding these limitations would significantly burden service providers in the short term until the conflict surrounding the subpoena provision is resolved, it would likely be a much more efficient approach in the long run. In addition, as will be suggested later in this Article, Congress could include an express provision in the DMCA requiring copyright owners to compensate service providers for unduly burdensome subpoenas, thereby shifting the financial burden at least somewhat back to the copyright owners.[223]

B. Constitutional Issues

In addition to the issues relating to the construction and interpretation of section 512, a number of constitutional challenges have been levied against the subpoena provision. These challenges have centered on Article III and the First and Fifth Amendments. Privacy advocates argue that the DMCA subpoena provision unconstitutionally implicates the rights to free speech and due process of law in addition to violating the Article III "case or controversy" requirement.[224]

1. Violation of the Article III Case or Controversy Requirement?

Article III, section 2 of the United States Constitution limits the exercise of federal judicial authority to situations involving "cases" or "controversies."[225] This restriction is generally interpreted to mean that federal courts may only resolve legal questions arising out of

[222] Fed. R. Civ. P. 45(b)(2) (articulating that Congress may provide for nationwide service of process in specific federal statutes, thus, overriding the geographical limitations of Rule 45); Motion to Enforce Subpoena to MIT at 15 (noting that Congress amended CERCLA to confirm that nationwide service of process was available under that statute).

[223] *See infra* Part V.D.

[224] *See* Brief of Amici Curiae in Support of Appellant Verizon Internet Services and Urging Reversal at 4, In re Verizon Internet Servs., Inc. Subpoena Enforcement Matter, Nos. 03-7015, 03-7053 (D.C. Cir. filed May 16, 2003) (consolidated appeal) [hereinafter Brief of Amici Curiae].

[225] U.S. CONST. art. III, § 2.

actual disputes between real parties.[226] In *Verizon II*, the ISP argued that the DMCA subpoena provision violates Article III because "it authorizes federal courts to issue subpoenas in the absence of a pending case or controversy."[227] Verizon maintained that "[a]n ex parte request for a subpoena duces tecum is not in itself a 'case or controversy' within the meaning of Article III" because it neither names an adverse party nor seeks any form of judicial relief or decree.[228] Because "the power to issue subpoenas exists only in the context of a case that is properly pending before a federal court," Verizon concluded that subpoenas issued pursuant to the DMCA are unenforceable under Article III.[229]

The court rejected each of Verizon's contentions based on several grounds. Initially, the court noted that "the clerk's issuance of a section 512(h) subpoena does not involve either the exercise of judicial power or the exercise by federal judges of…investigatory power," and thus could not be construed as an act of the court.[230] The court pointed out that the clerk exercises no discretion and merely executes a ministerial duty.[231] The court reasoned that the Supreme Court

---

[226] *See* Whitmore v. Arkansas, 495 U.S. 149, 154-55 (1990). In its brief in support of its motion to quash the second subpoena, Verizon defined "case or controversy" as an "adversarial proceeding seeking a judicial determination of an actual legal claim." Verizon Internet Services, Inc.'s Brief in Support of its Motion to Quash February 4, 2003 Subpoena and Addressing Questions Propounded by the Court at 4, *Verizon II* , 257 F. Supp. 2d 244 (D.D.C. 2003) (1:03MS00040-JDB) [hereinafter Verizon's Brief].

[227] *Verizon II*, 257 F. Supp. 2d at 248.

[228] Verizon's Brief at 9.

[229] *Id.* at 12. Verizon quoted the U.S. Supreme Court's opinion in *United States Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72 (1988):

> Federal Rule Civil Procedure 45 grants a district court the power to issue subpoenas as to witnesses and documents, but the subpoena power of a court cannot be more extensive than its jurisdiction. It follows that if a district court does not have subject-matter jurisdiction over the underlying action, and the process was not issued in aid of determining that jurisdiction, then the process is void and an order of civil contempt based on refusal to honor it must be reversed. *Id.* at 76.

[230] *Verizon II*, 257 F. Supp. 2d at 249.

[231] *Id.* at 249-50 (finding support for this argument in the legislative record in S. REP. NO. 105-190, at 51).

has long "distinguished between actions that are ministerial in nature and those that constitute an exercise of judicial, legislative, or discretionary executive power."[232] Quoting Justice Marshall's opinion in *Custiss v. Georgetown & Alexandria Turnpike Co.*, the court stated that "the legislature may direct the clerk of a court to perform a specified service, without making his act the act of the court."[233] From a practical perspective, reasoned the court, no Article III judge takes any action with respect to a DMCA subpoena until the copyright owner moves to enforce it or the service provider moves to quash it.[234] Once either of these actions occurs, an actual controversy exists sufficient to confer jurisdiction under Article III.[235]

Verizon expressly opposed this reasoning, arguing that subpoenas are issued in the name of the court and should be treated as acts of the court.[236] In response, the court held that there is a distinction between subpoenas issued by express order of a judge and subpoenas issued by the clerk of the court.[237] The court found that this distinction supported the view that the issuance of a subpoena by a clerk of the court is merely "a ministerial task accomplished without judicial involvement…"[238]

---

[232] *Id.* at 250 (citing Custiss v. Georgetown & Alexandria Turnpike Co., 10 U.S. 233, 237 (1810)).

[233] *Id.* (quoting *Custiss*, 10 U.S. at 236).

[234] *Id.*

[235] *Id.*

[236] *Verizon II*, 257 F. Supp. 2d at 250.

[237] *Id.* at 251 (finding support for this distinction in Fed. R. Civ. P. 45 and Waste Conversion, Inc. v. Rollins Envtl. Servs., Inc., 893 F.2d 605, 608 (3d Cir. 1990)).

[238] *Id.*

The court further stated that even if the issuance of a DMCA subpoena could be characterized as a judicial act, Verizon's Article III challenge would still fail for two reasons.[239] First, "Congress has enacted several provisions that specifically authorize the clerk of the district court to issue subpoenas despite the absence of a pending case or controversy in the federal courts."[240] Second, aside from the subpoenas authorized in these provisions, "'federal courts and judges have long performed a variety of functions that…do not necessarily or directly involve adversarial proceedings within a trial or appellate court."[241] The court drew an analogy to Rule 27(a) of the Federal Rules of Civil Procedure, which allows a court to order the deposition of a witness before an action is filed, where doing so would "prevent a failure or delay of justice."[242] Under both of these provisions, "private parties may avail themselves of judicial machinery to obtain information prior to the filing of a complaint…if they satisfy a specific set of criteria and identify with particularity the information they seek to compel."[243]

In its supporting brief, Verizon rejected this analogy, which was indirectly raised by the RIAA.[244] Verizon noted that Rule 27(a) requires a demonstration that the petitioner for such an order expects to be a party to an action that it is presently unable to bring or cause to be

---

[239] *Id.*

[240] *Id.* (citing, among other statutes, 2 U.S.C. § 388 (2000) ("subpoenas for depositions in connection with proceedings in the House of Representatives"); 35 U.S.C. § 24 (2000) ("subpoenas for evidence to be used in connection with proceedings in Patent and Trademark Office"); 45 U.S.C. § 157(h) ("subpoenas at the request of arbitrators under the Railway Labor Act")).

[241] *Id.* at 251-52 (quoting Morrison v. Olson, 487 U.S. 654, 681 n.20 (1988)). The court noted that in the criminal context, courts both issue warrants and review applications for surveillance, which requires judicial involvement and discretion in an ex parte proceeding. *Id.* at 252. Courts are also authorized "to require testimony or evidence for use in a foreign tribunal, even where no proceeding is yet pending in that forum." *Id.*

[242] *Id.* at 252 (quoting Fed. R. Civ. P. 27(a)(3)).

[243] *Id.* at 253.

[244] Verizon Brief at 14.

brought.[245] Section 512(h) contains no similar intent to file suit requirement, which makes it less certain that the judicial action in issuing a DMCA subpoena would relate to an actual action in federal court.[246] Indeed, Verizon pointed out that the RIAA has expressly stated that it "merely wishes to contact and admonish individual subscribers it suspects of copyright infringement and would prefer not to file suit against them."[247] The court, however, dismissed Verizon's argument on this point, stating that section 512(h)'s requirement of a sworn declaration that the information to be obtained will only be used for the purpose of protecting copyrights is sufficiently similar to the Rule 27(a) requirement as to render Verizon's distinction between the two provisions inconsequential.

While Verizon's arguments raise legitimate theoretical Article III issues with respect to the DMCA subpoena provision, this is likely to be an unsuccessful basis for future constitutional challenges. As the *Verizon II* court pointed out, there are a significant number of similar provisions in existence that have passed Article III muster.[248] The strongest argument in support of an Article III challenge is that section 512(h) is unique in allowing "a broad category of *private* actors to obtain sensitive information from third parties, outside the context of litigation."[249] Such private use of the courts nearly always occurs in the context of actual or

[245] *Id.* at 14-15 (citing Fed. R. Civ. P. 27(a)(3)).

[246] *Id.* at 15.

[247] *Id.* (citing RIAA Reply Brief in Support of Motion to Enforce at 12-14, *Verizon I*, 240 F. Supp. 2d 24 (D.D.C. 2003)).

[248] *Verizon II*, 257 F. Supp. 2d at 251-52.

[249] Davidson, *supra* note 27 (emphasis in original).

pending litigation and under the supervision of a judge.[250] An argument emphasizing this point might be somewhat more successful than the approach taken by Verizon.

Another obstacle to the successful challenge of the DMCA subpoena provision on Article III grounds is the fact that there is essentially only one other solution to this problem, which is not entirely practical. That solution, which Verizon raised as a possible alternative in the first case, would be to require copyright owners to bring "John Doe" actions before they could subpoena alleged infringers' subscriber information.[251] This approach would require copyright owners to file anonymous lawsuits before they would be able to discover alleged infringers' identities.[252] The court rejected this possible approach to the Article III problem on the grounds that there was no support for it either in the text or the legislative history of the DMCA.[253] The court held that requiring such a procedure would defeat the major purpose of the statute, which is the expeditious protection of copyrights.[254] In addition, the court found that such a procedure would be unduly burdensome on copyright owners and would not necessarily be any more protective of the rights of alleged infringers.[255]

Although the DC Circuit never reached this constitutional issue on appeal, its decision to disallow section 512(h) subpoenas in situations where the service provider is merely a passive conduit for the transmission of infringing materials has effectively forced copyright holders to begin bringing John Doe suits. Since the Court of Appeals rendered its decision in December

[250] *Id.*

[251] *Verizon I*, 240 F. Supp. 2d at 39.

[252] *Id.*

[253] *Id.* at 40.

[254] *Id.* (holding that such a procedure would result in delays that would be at odds with Congress's design for the DMCA).

[255] *Id.* at 40-41.

2003, the RIAA has ceased issuing section 512(h) subpoenas.[256] Determined to continue enforcing their rights under the law, copyright holders have resorted to bringing suits against anonymous infringers and using traditional subpoenas to discover offenders' identities within the context of litigation.[257]

Due to the extremely rapid nature in which copyrighted songs are illegally disseminated on P2P networks, John Doe suits are not an appropriate remedy for copyright holders. Forcing a copyright holder to engage in costly and time-consuming litigation while the defendants continue to anonymously share infringing materials with millions of other individuals is distinctly unfair and contrary to Congressional intent. As the *Verizon I* court pointed out, Congress intended for copyright holders to have an efficient and expeditious tool for uncovering and halting infringement, which John Doe suits are not.[258] As will be discussed shortly, a subpoena process with built-in statutory protections would afford copyright owners with a remedy much more suited to the problem posed by P2P networks while providing adequate protection for the rights of alleged infringers. Ironically, offenders currently facing John Doe lawsuits would likely prefer the section 512(h) subpoena process, which typically resulted in minimal settlements with copyright holders, to full-blown lawsuits, which will no doubt result in much stiffer penalties.

It remains to be seen how other jurisdictions will rule on whether DMCA subpoenas violate Article III. Although the issue is moot with respect to subpoenas issued in the District of Columbia for the identities of P2P file sharers, it remains an open question in the remaining eleven circuits where DMCA subpoenas issued based on infringement falling under section

---

[256] *RIAA Subpoenas Halted*, Electronic Frontier Foundation (Dec. 1, 2003), *at* http://www.eff.org/IP/P2P/riaasubpoenas/ (last visited Feb. 17, 2004).

[257] *Id.* (noting that the RIAA has filed John Doe suits against 532 unidentified alleged infringers).

[258] *Verizon I*, 240 F. Supp. 2d at 40.

512(a) are still valid. Even if the other jurisdictions follow the lead of the DC Circuit in disallowing section 512(h) subpoenas in situations where the service provider is merely a passive conduit for the transmission of infringing materials, subpoenas issued in cases governed by subsections (b) through (d) may still violate Article III. However, because there is analogous precedent for subsection 512(h) and because there are no truly viable alternatives, Article III challenges to the DMCA subpoena provision will likely continue to be unsuccessful.[259]

2. Violations of the First Amendment Right to Free Speech and the Fifth Amendment Guarantee of Federal Due Process?

Verizon, backed by a veritable throng of amici curiae supporters, also challenged the DMCA subpoena provision on First and Fifth Amendment grounds in the second Verizon case.[260] Verizon contended that the statute provides insufficient procedural protection against the subpoena provision's intrusion on the right to free anonymous speech.[261] Verizon argued that, as interpreted by the RIAA and the *Verizon I* court, the subpoena provision is "vastly overly broad" and should be held invalid.[262]

Discussing a line of recent decisions, Verizon noted that the U.S. Supreme Court has "repeatedly recognized that individuals have a right to speak, listen, and associate anonymously"

[259] Pacific Bell Internet Services has raised essentially the same Article III issue in its declaratory action against the RIAA and other copyright owners pending in the Northern District of California. *Pacific Bell Internet Servs. v. Recording Indus. Ass'n of America*, No. C 03-3560 SI (N.D. Cal. filed July 30, 2003). A conflicting opinion would not be altogether surprising from the Ninth Circuit, which is commonly in disagreement with other jurisdictions.

[260] *Verizon II*, 257 F. Supp. 2d at 257.

[261] Verizon Brief at 19. Verizon's argument combines the First and Fifth Amendment issues. Essentially, the subpoena provision deprives alleged infringers of their First Amendment right to free, anonymous speech without affording them the due process of law guaranteed by the Fifth Amendment. *Id.*

[262] *Id.*

in numerous situations.[263] Such free and anonymous expression extends to the context of the Internet.[264] Verizon acknowledged that "there is no First Amendment right to engage in copyright infringement."[265] However, Verizon argued, the subpoena provision has the power to strip away a user's right to anonymity in other contexts.[266] In addition, section 512(h) does not include any "built-in safeguards" against the curtailment of free, anonymous speech in these other contexts.[267] Essentially, Verizon argued that although there is no right to free, anonymous speech in the infringement of copyrights, there is a right to free, anonymous speech in other legitimate online activities, and, in uncovering the identity of a user to establish infringement, the DMCA subpoena provision deprives an alleged infringer of the right to speak anonymously in any context. Without sufficient statutory safeguards to protect against the improper or mistaken revelation of a subscriber's identity, the subpoena provision is unconstitutionally broad. In depriving an individual of such a fundamental right, the subpoena provision merely requires "an *ex parte* 'good faith' allegation by anyone willing to allege he or she is a copyright owner, or authorized to act on behalf of a copyright owner, and that copyright infringement *might* be occurring."[268] Such measures are not enough to protect the right of free, anonymous speech, Verizon argued. Verizon noted that the lack of an adversarial process was the primary

[263] *Id.* at 19-20 (citing Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 122 S. Ct. 2080, 2089 (2002); Buckley v. American Constitutional law Found., Inc., 525 U.S. 182, 200, 204 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995)).

[264] *Id.* at 20 (citing Reno v. ACLU, 521 U.S. 844, 870 (1997)).

[265] *Id.* at 24.

[266] *Id.* at 24-25.

[267] *Id.* at 25.

[268] *Id.* (citing § 512(c)(3)(A)(v)).

deficiency in the DMCA subpoena provision.[269] This deficiency "will inevitably lead to both honest mistakes and deliberate abuse—thereby stripping Internet users of anonymity even where the underlying speech and association is fully protected."[270] In support of its argument, Verizon cited an instance of mistake that had already occurred, which will be discussed later in this Article in conjunction with an assortment of other mistakes and abuses that have occurred recently under the authority of section 512(h).[271]

Not surprisingly, considering its holding in *Verizon I*, the *Verizon II* court rejected these First and Fifth Amendment arguments and upheld the constitutionality of the DMCA subpoena provision.[272] As a preliminary matter, the court acknowledged that Verizon had standing to assert these constitutional challenges on behalf of its subscribers.[273] The court also acknowledged that the Supreme Court has recognized a right of anonymity within the First Amendment and that the protections of that right extend to expression on the Internet.[274] In addition, the court noted that there are some limitations on subpoena power "when its invocation affects First Amendment rights involving anonymity."[275] The court found it significant, however, that the U.S. Supreme Court's holdings that the First Amendment protects anonymity have been rendered in the context of cases involving "core" First Amendment expression, such

[269] *Id.* at 26.

[270] *Id.*

[271] *Id.* at 27; *see infra* notes 288-91 and accompanying text.

[272] *Verizon II*, 257 F. Supp. 2d at 257. In *Verizon I*, Judge Bates informally addressed the First Amendment issue, concluding that it was unlikely that the DMCA subpoena provision violated the right to free speech in an unconstitutional manner. *Verizon I*, 240 F. Supp. 2d at 42-44.

[273] *Verizon II*, 257 F. Supp. 2d at 258.

[274] *Id.* at 258-59 (citing *Buckley*, 525 U.S. at 200; *Reno*, 521 U.S. at 870).

[275] *Id.* at 259, n.17.

as religious or political speech.[276] The court found that the DMCA subpoena power "does not directly impact core political speech, and thus may not warrant the type of 'exacting scrutiny' reserved for that context."[277] The court concluded that although some First Amendment protection should be afforded to anonymous expression on the Internet, the degree of that protection "is minimal where alleged copyright infringement is the expression at issue."[278]

In addition, the court found that section 512(h) affords alleged infringers sufficient procedural safeguards to protect their First Amendment rights.[279] The court pointed to the fact that to obtain a section 512(h) subpoena, one must provide: (1) a statement that the use of copyrighted material is not authorized by the owner and that the information in the notification is accurate,[280] (2) 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 copyrights,[281] and (3) a statement, made under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of the infringed copyright.[282] Also, § 512(f) further discourages the abuse of subpoenas by providing for a cause of action against anyone who "knowingly materially misrepresents" that activity is infringing.[283]

---

[276] *Id.* at 259-60 (quoting Roth v. United States, 354 U.S. 476, 484 (1957), "The First Amendment affords the broadest protection to such political expression in order 'to assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'").

[277] *Id.* at 260 (citing McIntyre v. Ohio Election Comm'n, 514 U.S. 334, 347 (1995)).

[278] *Verizon II*, 257 F. Supp. 2d at 260.

[279] *Id.* at 262.

[280] *Id.* (citing § 512(c)(3)(A)(v)).

[281] *Id.* (citing § 512(h)(2)(C)).

[282] *Id.* (citing § 512(c)(3)(A)(vi)).

[283] *Id.* at 263 (citing § 512(f)).

Holding that these procedural safeguards sufficiently protect alleged infringers against baseless or abusive subpoenas, the court concluded that "it is unlikely that section 512(h) will require disclosure, to any significant degree, of the identity of individuals engaged in protected anonymous speech, as opposed to those engaged in unprotected copyright infringement."[284]

Finally, despite acknowledging that section 512(h) will impact some protected expression and that the provision could be used to mistakenly pursue and obtain the identity of an innocent user, Judge Bates concluded that section 512(h) is not so "substantially" overbroad that it may be invalidated on its face.[285] He found it significant that Verizon never introduced evidence of abuse or mistake in the use of the DMCA subpoena provision during the five years since its enactment.

Unfortunately, Judge Bates's opinion in *Verizon II* contains several major holes and he ignored important practical considerations regarding the DMCA's operation. First, "all these protections" cited by Judge Bates are not necessarily sufficient to protect the First Amendment rights of alleged infringers. He listed three requirements for obtaining a subpoena pursuant to the DMCA; however, each of these three requirements depends solely on the conscience of the party attempting to obtain the subpoena. Two of them merely demand statements made in good faith. Although the third requirement demands a statement made under penalty of perjury, the slim chance that a U.S. Attorney will choose to prosecute such an offense is likely to have very little deterrent effect.[286] There is no step in the subpoena provision that allows for independent verification of the statements made by the party seeking the subpoena before it is issued.

---

[284] *Id.*

[285] *Id.* at 264 ("[T]he overbreadth of a statute must not only be real, but substantial as well."); Ashcroft v. ACLU, 535 U.S. 564, 584 (2002) ("Only a statute that is substantially overbroad may be invalidated on its face.").

[286] *See* Davidson, *supra* note 27.

Additionally, each of these safeguards listed by Judge Bates only protects against the *abuse* of the DMCA subpoena power. They do nothing to prevent the release of identification information in response to a subpoena issued based on a *mistake* made in good faith. Section 512 supplies a procedure for challenging mistaken takedown notices;[287] such a procedure is even more crucial in the subpoena context because identification information cannot be unlearned or returned once it is received. An appropriate challenging mechanism would not involve anything as burdensome as a full evidentiary hearing, but would only require that some minimal independent assessment of the validity of the subpoena request be made, possibly by the service provider or the clerk of the issuing court.

A second flaw in Judge Bates's opinion lies in his disregard for the substantial potential for overbreadth posed by the DMCA subpoena provision. Not finding any evidence of abuse or mistakes in the subpoena provision's short history, he essentially concluded that such a risk is minimal.[288] There have occurred already, however, instances of mistakenly issued subpoenas and subpoena responses.[289] For example, MIT finally released to the RIAA the name and information of a student with whom it associated the IP address listed on the subpoena issued by the RIAA. "Despite having been out of the country at the time of the alleged infringement and declaring that he did not even own a computer, the student was unable to prevent release of his name and identifying information."[290] In another case, "seven record labels mistakenly sued a

[287] 17 U.S.C. § 512(g) (2000).

[288] *Verizon II*, 257 F. Supp.2d at 265.

[289] *Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands*, Electronic Frontier Foundation (Oct. 7, 2003), (citing Keith J. Winstein, *MIT Names Student as Alleged Infringer*, The Tech (Sept. 9, 2003); Chris Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sept. 24, 2003), *at* http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php (last visited Feb. 17, 2004).

[290] *Id*.

65-year-old Massachusetts woman for copyright infringement…based only on KaAaA screenshots and Comcast's disclosure of her name and address in response to a subpoena."[291] The woman, however, only used a Macintosh computer, which cannot support the KaZaA program.[292] Clearly, contrary to Judge Bates's opinion, mistakes have occurred and will continue to occur as long as the subpoena provision operates as it currently stands, thus, resulting in the improper deprivation of First Amendment rights.

Judge Bates's reasoning also ignores the fact that the subpoena provision has experienced extremely limited use until very recently. Copyright owners have primarily utilized the takedown notification process throughout most of the DMCA's short life.[293] These takedown notifications have achieved notoriety for their frequent mistakes and often frivolous and harassing nature. A glance at the Electronic Frontier Foundation's website confirms that this reputation is indeed deserved.[294] It contains multiple documented instances of takedown notifications issued mistakenly or for purposes of harassment.[295] The takedown provisions contain even more safeguards than the subpoena provision, yet it is still vulnerable to frequent mistakes and misuse. Evidently, the safeguards that Judge Bates listed in his opinion are not sufficient to protect the subpoena provision from infringing on users' First Amendment rights in an overbroad manner. Section 512 is in dire need of additional procedural safeguards that would

---

[291] *Id.*

[292] *Id.*

[293] *See supra* note 96 and accompanying text.

[294] *Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands*, Electronic Frontier Foundation, *at* http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php (last visited Feb. 17, 2004).

[295] *Id.* "The RIAA recently admitted to several dozen additional errors in sending accusatory DMCA notices—all made in a single week." *Id.* (citing McCullagh, *supra* note 111).

protect users from erroneous identification without unduly burdening copyright owners in their quest to pursue and put an end to infringement.

C. Practical Policy Issues: The Subpoena Provision's Negative Potential

In addition to these constitutional and statutory issues that have been propounded with respect to the DMCA subpoena provision, various practical concerns have been raised regarding its application. Privacy advocates are quick to note the number of erroneous takedown notifications and subpoenas that have been issued under the DMCA.[296] Descriptions of worst-case scenarios that could arise as a result of abuse of the subpoena provision abound. However, even a well-functioning subpoena process would inherently possess some potential for mistakes and abuses. A well-functioning subpoena process could also impose significant burdens, both legally and administratively, on all the parties involved, especially in the event that a large number of subpoenas are issued. Several questions arise in connection with the management of these negative consequences, but only two will be discussed in this Article. First, who should bear the burden of responding to masses of subpoenas? Also, who should bear the burden of discovering and compensating for the mistakes and abuses that will inevitably occur?

1. Undue Response Burden

In answer to the first question, it may be more appropriate and efficient to shift at least some of the burden of responding to the potential flood of DMCA subpoenas back to the copyright owners. In the current battle against copyright infringement, there are many copyright owners from a broad range of backgrounds pursuing a host of online copyright infringers.[297] The

---

[296] *Id.*

[297] *Id.* ("In 2002, Pacific Bell Internet Services and its affiliates were given more than 16,700 DMCA notices by RIAA agent MediaForce; in July 2003, RIAA attempted to serve more than 200 subpoenas through various affiliated entities. Titan Media, a purveyor of pornographic materials, sent a single subpoena demanding identities of alleged infringers at 59 different dynamically assigned IP addresses, then dropped the subpoena when Pacific Bell announced its intent to challenge its enforcement."). In addition to members of the recording and motion picture

incredibly large number of parties involved could result in a landslide of subpoenas that would overrun smaller ISPs.[298] It takes a service provider employee approximately 20 minutes to research and respond to a subpoena request.[299] Multiplying this time expenditure by the thousands of potential subpoenas—not simply from the music recording industry, but also from many other types of copyright owners—results in significant potential expense for service providers. Not only would the administrative burden of responding to each subpoena be overwhelming, but the potential legal burden stemming from fighting a subpoena or defending an action for improper release of identification information could also be enormous. Smaller service providers generally have minimal administrative staffing and no legal department. The burden that would be caused by a flood of subpoenas would crush many of these smaller ISPs out of existence.

The problem with the current process is that there are no limiting factors that would provide some control over the number of subpoenas that are issued. First, the identification of infringers and the request for subpoenas is an almost completely automated process for copyright owners, which means that they bear little burden or cost at the front end that would limit the number of subpoenas requested.[300] Second, there are no requirements on what a copyright owner

---

industries, software distributors and a host of independent writers and artists have utilized the DMCA, whether wrong or right, to protect their copyrights.

[298] *District of Columbia Court Lacks Authority to Issue DMCA Subpoenas to Boston Schools*, 66 ELECTRONIC COM. & L. REP. No. 1634, at 459 (Aug. 15, 2003); *Issues Arising out of RIAA v. Verizon*, Electronic Privacy Information Center (Dec. 19, 2003) (noting the general concern "that as copyright holders chase after hundreds or even thousands of peer-to-peer users using automated copyright infringement monitors, such as Ranger Inc., it will result in huge costs for the ISPs faced with processing the requests"), *at* http://www.epic.org/privacy/copyright/verizon/ (last visited Feb. 17, 2004).

[299] Bob Liu, *Copyrights: More Work, More Headaches*, Internet.com (March 12, 2003) (noting that a network administrator at a university with only 5,500 students requires 15 to 30 minutes to find the source of the copyright infringement upon receiving a complaint), *at* http://isp-planet.com/perspectives/2003/bliu.html (last visited Feb. 17, 2004).

[300] *See* Manjoo, *supra* note 37 (quoting Peter Swire, law professor at Ohio State University).

must do once he has obtained an alleged infringer's identification information.[301] Requiring a copyright owner to pursue an action or to at least further investigate the matter would ensure that the copyright owner only requests subpoenas in situations where infringement is at least somewhat certain. Because there is no such requirement that any kind of legal or investigative action be taken, there are no practical limitations at the tail end of the process either. Finally, there is no provision for shifting the cost of improperly issued subpoenas back to copyright owners. Such a provision would decrease the number of mistakenly issued subpoenas by providing copyright owners with incentive to request subpoenas only in situations where they are fairly certain that infringement is indeed occurring.

Essentially, the current process unfairly distributes the entire burden of responding to subpoenas to ISPs in a manner that is contrary to the legislature's intent in enacting section 512. While Congress intended to make the enforcement process as fast and efficient as possible for copyright owners,[302] this goal is not sacrificed by forcing copyright owners to bear some of the administrative costs that responding to subpoenas imposes. Especially in the event of mistakenly issued subpoenas, over which service providers have no control, such a burden shifting scheme would seem appropriate and much more efficient. It must be remembered that the other primary goal of section 512 is to clarify and limit the liability of service providers for their subscribers' infringement.[303] From a monetary perspective, the burden of responding to a flood of subpoena requests could serve as much of a penalty as would a finding of liability for infringement, thus defeating one of the major goals of the DMCA. Congress made it clear that section 512 was

---

[301] *See* Davidson, *supra* note 27.

[302] *Verizon I*, 240 F. Supp. 2d at 35 (citing S. REP. NO. 105-190, at 8).

[303] S. REP. NO. 105-190, at 19-20

intended to foster cooperation between service providers and copyright owners in the fight against infringement.[304] Such legislative intent should not be arbitrarily limited to exclude financial cooperation.

2. Undue Burden of Identifying and Correcting Erroneous Subpoenas

Similarly, the entire burden of discovering abusive and erroneous DMCA subpoenas also falls squarely on the shoulder of ISPs and their subscribers. The RIAA claims that it individually checks each subpoena request before it is sent to the clerk of the court, but obviously mistakes slip past their inspection process.[305] The burden of catching these missed mistakes subsequently falls on the service providers. If the service provider chooses not to respond to an erroneously issued subpoena, it must move to quash it in court and bears the cost for doing so. If the service provider simply responds to the erroneous subpoena, as the DMCA requires, the service provider may open itself up to potential liability.[306] In either event, the service provider bears the burden of not only discovering the copyright owner's mistake, but also correcting it. This inequitable result could be remedied with the incorporation of a provision in section 512 that requires copyright owners to compensate service providers for any costs associated with challenging erroneously issued subpoenas.

By no means does this Article purport to discuss every issue that has been raised with respect to the DMCA subpoena provision, but these represent most of the more compelling

---

[304] S. REP. NO. 105-190, at 20.

[305] *See* Lyman, *supra* note 31 (outlining the RIAA's approach to uncovering infringers); Manjoo, *supra* note 37 (quoting Cindy Cohn, legal director of the Electronic Frontier Foundation, "The ISPs get thousands of these things, and they get a not insignificant percent that are not just wrong, but are spectacularly wrong. And if the Verizon decision under 512(h) is upheld, we'll start seeing the same thing for people's identities, and they're going to be wrong in the same percentage that they're wrong now.").

[306] Nothing in section 512 appears to protect the service provider in this situation since section 512(f)(1) seems only to apply to incorrect takedowns, not subpoena responses.

challenges. Next, Part V proposes various changes that could be introduced to section 512, which would alleviate many of these problems.

V. PROPOSED AMENDMENTS TO THE DMCA SUBPOENA PROVISION

The fact that so many challenges have been levied against the DMCA subpoena provision and so many practical issues have been raised with respect to its application makes it exceedingly clear that the subpoena provision, in its current state, is significantly flawed. These flaws were not a major concern until recently, when they became magnified as a result of copyright owners' sharply increased utilization of the provision. Rather than simply discarding the subpoena provision, however, a better approach would be to augment it with additional procedural privacy protections.

A. Subscriber Notice

The issuance of formal notification to subscribers before their identity is revealed would provide them with warning and would allow them to contest wrongfully issued subpoenas. Such notice would come from the service provider and would likely arrive in the form of an e-mail to streamline the process as much as possible. Several state statutes require that service providers afford notice to an anonymous subscriber at least a certain period of time before they may release the subscriber's identity to the subpoenaing party.[307] A notice requirement would preserve the

[307] *See e.g.*, VA. CODE § 8.01-407.1 (2000).

> "Except where the anonymous communicator has consented to disclosure in advance, within five business days after receipt of a subpoena and supporting materials calling for disclosure of identifying information concerning an anonymous communicator, the individual or entity to whom the subpoena is addressed shall (i) send an electronic mail notification to the anonymous communicator reporting that the subpoena has been received if an e-mail address is available and (ii) dispatch one copy thereof, by registered mail or commercial delivery service, return receipt requested, to the anonymous communicator at his last known address, if any is on file with the person to whom the subpoena is addressed."

Id. § 8.01-407.1(A)(3).

due process rights of Internet users and would also act as a deterrence to abusive subpoena requests.[308] Such notice would also increase the public's awareness of the legal actions that copyright owners are bringing against infringers, which would result in a further deterrent effect.[309] Finally, the provision of notice to subscribers would not disrupt the investigation or enforcement process because the copyright owners would already have sufficient evidence of the infringement by the time the user is informed of the subpoena.[310]

While the requirement of such notice would cost copyright holders precious time, the subpoena could be served in conjunction with a takedown notification to the service provider or the subscriber, depending on where the infringing materials are located.[311] Such a measure would prevent any infringing material from being made available to other users while the enforcement is pending. In the case of infringing files located directly on the alleged infringer's computer, the suspect would be warned to disable online access to them. If the suspect refused to cooperate, his or her service could be terminated until the issue is resolved.

B. Restrictions on Retention and Use of Subpoenaed Information

To some extent, section 512 purports to restrict the manner in which subscriber identity information can be used.[312] Such restrictions, however, could be more explicitly clarified, and a specific limit could be placed on the time period for which identity information could be

[308] *See* Davidson, *supra* note 27.

[309] *Id.*

[310] *Id.*

[311] As noted by the DC Circuit in *Verizon*, because service providers do not have control over the infringing material being shared over P2P networks, such a situation would require the takedown notification to be issued directly to the offender. Such action would obviously require a change in the current law, which has no such provision.

[312] The subpoena provision requires "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." § 512(h)(2)(C). There are no built-in penalties for a violation of this requirement other than the possibility of prosecution for perjury, which is not necessarily the strongest deterrent.

retained.[313] Such a time limit would most appropriately be based on whether or not legal action is taken against the alleged infringer. For example, such a scheme could require that the information be erased within a period of 6 months after it is obtained if no suit is filed within that time. Otherwise, the information would have to be erased within a period of 6 months after the settlement or conclusion of a lawsuit and any resulting appeal.

These restrictions on content and duration would not hinder copyright owners using the subpoena process for legitimate enforcement purposes, but would go a long way to prevent identity information from being misused. Identity and contact information, especially in mass quantities, is extremely valuable today for advertising purposes. It is not inconceivable that a less than scrupulous copyright holder might sell a list of such information to an advertising agency or online business. Additionally, copyright holders could organize subpoenaed identity information to create infringer blacklists.[314] Those winding up on such a blacklist could find their names posted online or find themselves restricted from legitimately purchasing digital music recordings online. Specific restrictions on how copyright holders may use subpoenaed identity information and substantial penalties for their violation would ensure that such information is only used for the enforcement of copyrights and would help to alleviate legitimate public concern.

C. Private Right of Action for Abuse of Subpoena Process

Congress attempted to provide for penalties for abuse relating to section 512,[315] but further penalties are necessary to cover the broader range of situations that may currently arise in

[313] *See* Davidson, *supra* note 27.

[314] *Id.*

[315] *See e.g.*, § 512(f) (providing for the recovery of damages, including costs and attorneys' fees, incurred as a result of misrepresentation as to the infringing nature of material).

the context of copyright enforcement. In addition to providing a right of action against those materially misrepresenting infringement, such liability should also extend to service providers who do not provide notice to their subscribers and to copyright owners who misuse identification information. At least one state, California, has already begun considering similar legislation.[316] An extension of the penalties already provided for in section 512 would not burden parties using the subpoena authority for legitimate copyright enforcement, but would provide Internet users with recourse against abuses of the system.

Holding a service provider liable for failure to give notice to a subscriber that his or her identity has been subpoenaed places the burden of ensuring due process for the subscriber on the service provider. While this may seem somewhat harsh since the service provider is technically not even involved in the dispute, there is no other way to guarantee that the subscriber receives notice of the pending subpoena. The service provider is the only link between the copyright holder and the alleged infringer. As a result, there must be consequences for the failure to carry out the simple yet important task of conveying notice of a subpoena to the allegedly infringing subscriber.

D. Cost Reimbursement

Currently, the burden of responding to DMCA subpoenas falls entirely on ISPs. Shifting at least a portion of this burden back to copyright owners would not be inconsistent with the legislative intent behind section 512.[317] Requiring copyright owners to reimburse at least some of the costs associated with responding to subpoenas is also consistent with Rule 45 of the

[316] Internet Communications Protection Act of 2003, Cal. AB 1143 (2003).

[317] *See supra* note 302 and accompanying text.

Federal Rules of Civil Procedure and the subpoena provisions of several other federal statutes.[318] As discussed above, these costs have the potential to be significant, especially for smaller service providers. Section 512 currently does not provide any incentive, either negative or positive, to copyright holders to minimize these costs by ensuring the accuracy and appropriateness of their subpoena requests.

One reason for not statutorily shifting a portion of the subpoena response costs back to the copyright holders would be that service providers indirectly benefit, in the form of monthly service fees, from their subscribers' infringement. This logic falls apart to some extent, however, considering that most subscribers to Internet service would continue to use the Internet for other purposes regardless of their ability to download copyrighted material. Service providers do not receive any more or less benefit based on the type of online activity in which their subscribers engage.

On the other hand, the creation of some type of reimbursement scheme would likely reduce the number of frivolous, abusive, and erroneous subpoenas, thus rendering the entire process more efficient. If copyright holders knew that they would be subject to statutory fees or penalties for serving erroneous subpoenas or to liability for serving abusive or frivolous subpoenas, the issuance of an improper subpoena would likely be a much rarer occurrence. Statutorily shifting the cost of subpoenas in such cases would balance the burden of ensuring the accuracy of all subpoenas more evenly between service providers and copyright holders.

E. Reporting Requirement

One of the problems with section 512(h), which has resulted in significant public outcry against the DMCA, is that the public has little idea how often and for what purposes the

[318] *See* Fed. R. Civ. P. 45(c); 15 U.S.C. § 49 (2000) (Federal Trade Commission Act).

subpoena provision is being used.[319] An amendment to section 512(h) requiring an annual report to Congress on the number of subpoenas requested and granted and for what types of copyrighted material would provide the legislature with information that could be used to monitor for abuses and further streamline the subpoena process.[320] Such a requirement would also greatly allay the public's fear because much of that fear is of the unknown, rather than the subpoena process itself.

F. Putting it all Together

In a rather disjunctive fashion, this Article recommends a number of possible improvements to the DMCA subpoena provision. In concluding this discussion, it would likely be helpful to the reader to visualize how each of these improvements would work together to strengthen protection for the interests of both copyright holders and Internet users. The following hypothetical should assist the reader in this exercise.

Take the case of Bart and James, best friends and next door neighbors. Bart often uses his family's computer to illegally download copyrighted music files from a P2P program called SongsRus. Because James's parents have warned him not to download copyrighted music on their computer, he gets his daily dose of illegal audio entertainment at Bart's house. James, being an aspiring artist, has also drawn renderings of scenes from two recent motion pictures, which he saved on his computer in files titled after the movies. Not surprisingly, the local ISP, SpeedyCom, is subsequently served with subpoenas for the identities of both Bart and James by A1 Records and Big Hitz Entertainment, respectively.

---

[319] *See* Davidson, *supra* note 27.

[320] *Id.*

Assuming that these two subpoenas were not issued from a court in the DC circuit, under the current law, SpeedyCom would likely respond immediately to the subpoena pursuant to section 512(h), releasing both Bart's and James's identities (or their parents'). Unless SpeedyCom subsequently notified the families of the subpoenas and the release of their identities, neither family would even be aware of any trouble until contacted by the copyright holders or served with citation. Of course, the mistake made in James's case would be quickly discovered, but still too late to undo the release of his family's identity.

The proposals outlined in this Article, however, would require SpeedyCom to notify both Bart's and James's families *before* releasing their subscriber information. If SpeedyCom did not comply with this requirement, it would be liable to both families for damages and/or a statutory penalty.[321] Upon notification, each family would have the opportunity to present evidence to SpeedyCom as to why the subpoenas should not be answered. In James's case, SpeedyCom would simply pass this evidence onto Big Hitz Entertainment, and the mistake would be easily resolved. Big Hitz could be required to pay a statutory fee to SpeedyCom for the cost of handling the mistaken subpoena issuance. If, for some reason, Big Hitz still insisted that SpeedyCom respond to the subpoena, SpeedyCom could file a motion to quash in the court from which the subpoena was issued. Upon the court's granting of this motion, Big Hitz would be forced to reimburse SpeedyCom for the additional expense of protecting its subscriber.

In Bart's case, it is unlikely that evidence could be supplied to SpeedyCom as to why A1 Record's subpoena should not be answered. If Bart's family never responded with any such evidence or, upon evaluation of the evidence submitted, SpeedyCom determined that copyright infringement had indeed occurred, it would release the appropriate identifying information to A1

[321] Of course, damages would be much less, possibly even non-existent, in Bart's case due to the fact that he was in fact guilty of copyright violation.

Records and notify Bart's family accordingly. If SpeedyCom found some evidence suggesting that Bart had not engaged in copyright violation, it could again bring a motion to quash in the court from which the subpoena was issued. Upon the court's denial of this motion, SpeedyCom would be forced to reimburse A1 Records for the expense of enforcing the subpoena.

Suppose that Bart's family settles the dispute with A1 Records, but months later, A1 Records discovers that it can recoup some of the profits it has lost over the years to copyright infringement by selling all the identity information it has collected via DMCA subpoenas to an advertising or data collection agency. A1 Records feels that the annoying spam and sales calls that past infringers would receive after the sale of their information would serve them right. As it currently stands, section 512 does not provide recourse for Bart's family in this situation or penalties to be assessed against A1 Records for abuse of the subpoena process. If the proposals in this Article were implemented, Bart's family would have a private right of action against A1 Records. Such an action would be for the recovery of a statutory penalty, which would vary depending on the severity of the abuse.

This hypothetical situation highlights the major procedural shortcomings in the DMCA subpoena process and outlines a more equitable cost-balancing scheme, which would shift some of the burden of dealing with these subpoenas back to the copyright holders. This hypothetical also demonstrates the significant impact that implementing these relatively simple changes in the law would have.

VI. CONCLUSION

As the old saying goes, "If it ain't broke, don't fix it." Well, the DMCA subpoena provision is clearly "broke" and clearly requires fixing. Section 512(h) provides a very useful

and very necessary tool for copyright owners to combat online copyright infringement. Without such a provision, copyright owners would have no recourse against the actual perpetrators of infringement. Without there being any way for copyright owners to identify potential infringers, Internet users could continue engaging in copyright violation with impunity, hidden behind an impenetrable veil of anonymity. As it currently exists, however, section 512(h) threatens to tear down the entire curtain, exposing the identities of many innocent subscribers and depriving them of their fundamental Constitutional rights. This is an unacceptable result, even in the context of copyright enforcement. Section 512 could easily be amended to include the various procedural safeguards discussed above, which would protect the rights of individual users and alleviate the potential burden on ISPs, while continuing to afford copyright owners with an effective and expeditious mechanism for pursuing infringers.

Additionally, although enacted fewer than six years ago, section 512 is already in need of updating to bring it in line with current technology. In restructuring or redrafting the DMCA, Congress should give serious thought to simplifying section 512. In its current state, it is unduly specific and complicated, and thus does not afford copyright holders protection from the most serious form of infringement presently taking place. Legislation cannot anticipate tomorrow's technology today, but in simplifying section 512, Congress could make it much more likely that future forms of copyright infringement are covered under the next version of the DMCA.

As it currently stands, section 512 does not adequately protect the interests of copyright holders or Internet users. Rather than forcing the courts to legislate from their benches or allowing conflicting case law to sprout up across the country, Congress must act quickly to resolve the issues that have been raised with respect to the DMCA subpoena provision before too much damage is done. Unfortunately, while several legislators have raised outspoken challenges

to the provision, Congress appears deadlocked on how best to resolve these complicated issues. Thus, it may be some time before section 512 sees any substantive changes. Hopefully, the recent *Verizon* opinion will provide the impetus necessary to spur Congress to a speedier resolution. In the meantime, copyright infringement may decline, but so will the protection of copyrights and Internet users' fundamental constitutional rights.