NOTE

PRIVATE ENFORCEMENT OF THE DIGITAL MILLENNIUM COPYRIGHT ACT: EFFECTIVE WITHOUT GOVERNMENT INTERVENTION

Justin D. Fitzdam†

INTRODUCTION .......................................................... 1085
I. THE DIGITAL MILLENNIUM COPYRIGHT ACT .................. 1087
   A. The History of File Sharing and the DMCA ............. 1087
   B. Seven Years Later: Reflections on the DMCA .......... 1091
II. PRIVATE ENFORCEMENT OF THE DMCA ...................... 1095
   A. Initial Strategy: Going After the Corporate “Big
      Guns” ............................................................ 1095
   B. A New Approach: Attacking Individual Users ........ 1102
III. FEDERAL INVOLVEMENT IN DMCA ENFORCEMENT ......... 1104
IV. WHY INCREASED INSTITUTIONAL INVOLVEMENT IN DMCA
   ENFORCEMENT IS UNNECESSARY AND ALTERNATIVES FOR
   REQUIRED EFFECTIVE PRIVATE ENFORCEMENT ....... 1108
CONCLUSION ............................................................ 1116

INTRODUCTION

The creation of file sharing programs has led to an explosion in the number of electronic music files transferred over the Internet. These files, stored in the Moving Picture Experts Group Audio Layer 3 format (MP3), have become ubiquitous.

About half of the twelve to twenty-two year olds in the United States with internet access have downloaded copyrighted music files.¹ What once was tape-swapping practiced between friends is now an organized worldwide phenomenon. Each month, internet users exchange an estimated 400 million pirated music files.² The recording industry shipped 300 million fewer albums between 1999 and 2002 than it had in previous years.³ The recording industry reports that

† B.S., University of Florida, 2002; candidate for J.D., Cornell Law School, 2005; Note Editor, Volume 90, Cornell Law Review. I would like to thank Christopher Clark, Aileen Ocon, and Sean Thompson for investing countless hours editing this piece.

¹ See Steve Lohr, Fighting the Idea That All the Internet Is Free, N.Y. Times, Sept. 9, 2003, at Cl.
² See id.
³ Id.
Shipments continue to decrease at a rate of about fifteen percent annually.4

In response to these trends, Congress passed the Digital Millennium Copyright Act (DMCA) in 1998.5 The DMCA not only establishes liability for individuals who illegally transfer copyrighted music, but also establishes criteria by which to hold a company facilitating these transfers liable. Through the DMCA, the Recording Industry Association of America (RIAA) sought to stop the electronic transfer of copyrighted music between individuals.

At first, the RIAA attempted to shut down the individual services that facilitated many of the file transfers. Although this strategy worked initially,6 its ultimate effectiveness remains uncertain because of a federal circuit split over whether the creators of modern file sharing software are liable for its use in facilitating these transfers.7 The Supreme Court recently granted certiorari to resolve the dispute.8 In the meantime, the RIAA has implemented a new strategy by targeting individual users involved in MP3 swapping. This tactic involves filing mass lawsuits against users of file sharing programs such as Kazaa and Morpheus. For instance, in a September of 2003 set of filings, the RIAA sued 261 individuals allegedly involved in illegal file sharing,9 most of whom were college-age or younger.10

In addition to private enforcement, government agencies are also involved in the process. For example, the FBI is working with the RIAA to develop a warning seal similar to that seen on VHS tapes and DVDs.11 In June of 2003, Congress proposed the Piracy Deterrence and Education Act of 2003, an Act designed to increase the role of the

6 See A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1095 (9th Cir. 2002) (affirming the district court’s modified preliminary injunction and order “forcing Napster to disable its file transferring service until certain conditions are met to achieve full compliance with the modified preliminary injunction”).
7 Compare Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004) (holding that defendants are not liable for contributory and vicarious copyright infringement), cert. granted, 125 S. Ct. 686 (2004), with In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003) (finding that Internet website operators can be held liable for contributory and vicarious infringement), cert. denied, 540 U.S. 1107 (2004).
10 See id.
government in the enforcement process.\textsuperscript{12} Under this Act, the FBI would be responsible for detecting and notifying individuals allegedly participating in the transfer of copyrighted materials over the Internet.\textsuperscript{13} In addition, the FBI would be responsible for "facilitat[ing] the sharing among law enforcement agencies, Internet service providers, and copyright owners of information" relating to such behavior.\textsuperscript{14} Unfortunately, this proposed legislation is not the correct solution to the problem because it does not use government resources efficiently and it threatens individual electronic privacy.

Part I of this Note outlines the Digital Millennium Copyright Act, the statutory authority that permits the prosecution of illegal file sharing, and several criticisms of the Act. Part II discusses private attempts, such as those by the RIAA, to enforce these regulations. Part III analyzes and critiques the recent trend of increased government involvement in this process, such as the proposed Piracy Deterrence and Education Act of 2003. Finally, Part IV argues that Congress's proposed legislation is flawed and should not be enacted. Given the adequate remedies available through private enforcement, these measures are unnecessary, waste limited government resources, and raise privacy concerns.

I

THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. The History of File Sharing and the DMCA

The Internet was once an unregulated, "Wild West"\textsuperscript{15} electronic community. Proponents of this metaphor felt that the Internet, like the Wild West, "beckoned to the imagination as a place unregulated and uncivilized, whose inhabitants lived beyond the reach of law and the constraints of polite behavior."\textsuperscript{16} The Internet was attractive because of its inherent lawlessness\textsuperscript{17}—a principle a few courts even acknowledged. For example, in ACLU \textit{v. Reno}, the court commented that "the strength of the Internet is . . . chaos" and rested its holding on the theory that "the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects."\textsuperscript{18}

\begin{thebibliography}{9}
\item\textsuperscript{13} \textit{Id.} \S 3.
\item\textsuperscript{14} \textit{Id.} \S 3(2).
\item\textsuperscript{16} \textit{Id.} at 579 (quoting Ted Morgan, \textit{A Shovel of Stars: The Making of the American West 1800 to the Present} 13 (1995)).
\item\textsuperscript{17} \textit{Id.}
\end{thebibliography}
Congress does not find this analogy to be so promising, reasoning that the Wild West metaphor is a perfect argument for imposing new regulations.\textsuperscript{19} Congress asserts that regulation is necessary to protect businesses and citizens from this lawless frontier.\textsuperscript{20} Recently, Congress targeted the unauthorized electronic transmission of copyrighted materials, in part because of substantial pressure by the recording industry to constrain the widespread phenomenon of MP3 file sharing.\textsuperscript{21}

This recent phenomenon is largely attributable to advances in digital compression technology that facilitates the storage of audio recordings in small MP3 files.\textsuperscript{22} Although MP3 files are not perfect copies of the original audio recording, their small size make them well suited for transmission over the Internet.\textsuperscript{23} Individuals can acquire MP3 files in two ways. The first method is by using “ripping” software to extract and compress a digital copy of a compact disc (CD), which can then be stored on the user’s computer.\textsuperscript{24} Alternatively, an individual may download MP3 files from an internet file sharing service.\textsuperscript{25} In addition, increased Internet connection speeds and reduced computer storage costs have facilitated the ease of music file transfer.\textsuperscript{26}

There are a number of different types of file sharing services. Some services, such as the original Napster, operate through use of centralized servers.\textsuperscript{27} The file sharing program acquires a list of available MP3 files on the hard drives of individual users and conveys this information to other users who are searching for these files.\textsuperscript{28} If an individual wishes to download a file from a user, the service gives the acquiring individual’s computer the internet address of the person possessing the file.\textsuperscript{29} This, in turn, allows the individual’s computer to connect to the other user’s computer to transfer the file.\textsuperscript{30}

\textsuperscript{19} See Rusch, supra note 15, at 578.
\textsuperscript{20} See id. at 580.
\textsuperscript{23} See id. As a result of their small size, MP3 files can be quickly transferred between individuals. See id.
\textsuperscript{24} Id. “Ripping” is the term used to describe the extraction of audio files from a CD. Ripping may also be referred to as digital audio extraction (DAE). See id. at 373 n.9.
\textsuperscript{25} Id. at 373.
\textsuperscript{27} See id.
\textsuperscript{28} Id.
\textsuperscript{29} Id.
\textsuperscript{30} Id.
"Pure" peer-to-peer file sharing services, such as Kazaa, Morpheus, and Gnutella, operate without the use of a central server.\textsuperscript{31} When a user logs on to this service, he or she connects to other computers directly.\textsuperscript{32} The user’s computer then, without the aid of a centralized master list, searches all of the other users’ computers for the requested file.\textsuperscript{33} Thus, all data exchanges are solely between the individual computers.\textsuperscript{34}

In 1998, Congress responded to the increased swapping of copyrighted files by enacting the Digital Millennium Copyright Act.\textsuperscript{35} The DMCA was Congress’s attempt to modernize U.S. copyright law\textsuperscript{36} and was promulgated for two primary reasons: (1) to appease copyright owners’ fears that their material would be spread across the entire digital community,\textsuperscript{37} and (2) to affirm the ratification of the World Intellectual Property Organization (WIPO) treaties.\textsuperscript{38}

Title I of the DMCA implements the WIPO treaties in two ways.\textsuperscript{39} First, the DMCA prohibits the circumvention of copyright protection systems and provides that “[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work protected under this title.”\textsuperscript{40} The statute also bans the manufacture, sale, distribution, or trafficking of tools and technologies that make such circumvention possible.\textsuperscript{41} As a second means of incorporating the WIPO treaties, Title I also prohibits the removal of copyright management information.\textsuperscript{42} Certain organizations, such as nonprofit libraries and educational institutions, are exempt from some of the

\textsuperscript{31} See id.
\textsuperscript{32} Id.
\textsuperscript{34} Id.; see infra notes 101–02 and accompanying text.
\textsuperscript{37} See supra notes 1–4.
\textsuperscript{38} WIPO is an international organization with 181 member states dedicated to promoting the use and protection of intellectual property. The organization administers twenty-three international treaties that require member states to enforce certain copyright laws in their own countries. See World Intellectual Property Organization, About WIPO, at http://www.wipo.int/about-wipo/en/ (last visited Oct. 31, 2004). For a more thorough review of the WIPO treaties, see GRAHAM J H SMITH, INTERNET LAW AND REGULATION 15–16 (3d ed. 2002).
\textsuperscript{40} 17 U.S.C. § 1201(a) (2000).
\textsuperscript{41} Id. §§ 1201(a)(2), 1201(b).
\textsuperscript{42} See id.
provisions.\textsuperscript{43} Title I also imposes both civil and criminal liability on violators.\textsuperscript{44}

Title II of the DMCA is entitled “The Online Copyright Infringement Liability Limitation Act” and addresses the copyright liability of Internet Service Providers (ISPs).\textsuperscript{45} If an ISP complies with certain prerequisites, it will not be liable for monetary damages for various copyright infringement claims.\textsuperscript{46} Compliance also limits equitable and injunctive relief.\textsuperscript{47}

Title II specifically enumerates four limitations on ISPs liability. Section 512(a) addresses ISP liability for the transmission of infringing material over its network.\textsuperscript{48} Section 512(b) refers to liability for system caching, which in this sense refers to “the intermediate and temporary storage of material on a system or network” controlled by the ISP.\textsuperscript{49} Section 512(c) covers liability for copyrighted information that “resides on a system or network” controlled by the ISP.\textsuperscript{50} Finally, section 512(d) discusses liability for providing information location tools, such as directories, indexes, references, pointers, or hypertext links.\textsuperscript{51}

To qualify for any of these safe harbor provisions, the ISP must have a policy for terminating repeat offenders and notify account holders of this policy.\textsuperscript{52} The ISP must also accommodate and not interfere with “standard technical measures,” defined as those measures “used by copyright owners to identify or protect copyrighted works.”\textsuperscript{53} Some of the specific safe harbors have additional requirements. For example, to avoid liability under sections 512(c) and 512(d), the ISP must not have actual knowledge of the infringement or be “aware of facts or circumstances from which infringing activity is apparent.”\textsuperscript{54} In addition, the ISP must not receive direct financial benefits from the infringing activity.\textsuperscript{55} Further, to avoid liability under sections 512(b), 512(c), and 512(d), the ISP must be able to remove or prevent access to material claimed to be in violation of the DMCA.\textsuperscript{56}

\textsuperscript{43} Id. \S 1201(d).
\textsuperscript{44} Id. \S\S 1203, 1204.
\textsuperscript{45} This is a broad category, which includes Internet ISPs (ISPs), Online ISPs (OSPs), search engines, portals, and even owners of corporate intranets. See Ian C. Ballon, Internet and Electronic E-Commerce Law: A Primer, 1997 PLI/Corp 431, 474–75 (2003).
\textsuperscript{46} Id. at 475.
\textsuperscript{47} Id.
\textsuperscript{48} 17 U.S.C. \S 512(a) (2000).
\textsuperscript{49} See id. \S 512(b)(1).
\textsuperscript{50} Id. \S 512(c)(1).
\textsuperscript{51} Id. \S 512(d).
\textsuperscript{52} Id. \S 512(i)(1)(A).
\textsuperscript{53} Id. \S 512(i)(2).
\textsuperscript{54} Id. \S 512(c)(1)(A)(i)-(ii), (d)(1)(A)-(B).
\textsuperscript{55} Id. \S 512(c)(1)(B), (d)(3).
\textsuperscript{56} Id. \S 512(b)(2)(E), (c)(1)(c), (d)(3).
In addition to limiting the liability of ISPs, Title II also adds another important provision. Section 512(h) provides that "[a] copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to [an ISP] for identification of an alleged infringer in accordance with this subsection." To receive the subpoena, the affected party must file: (1) a copy of the Section 512(c) notice, (2) a proposed subpoena, and (3) a sworn declaration. Upon receipt of the subpoena, the service provider must "expeditiously disclose . . . information sufficient to identify the alleged infringer."

B. Seven Years Later: Reflections on the DMCA

Although the DMCA may aid in limiting the illegal distribution of copyrighted materials over the Internet, critics argue that the Act does so by sacrificing other legitimate interests. For example, critics claim that the DMCA impinges on free speech and allows copyright owners to override fair use rights.

Those who feel that the DMCA restricts free speech have compelling stories to support their argument. The case of Dmitry Sklyarov is a useful example. Sklyarov was a Russian programmer who worked for a company called ElcomSoft. While working at Elcomsoft, Sklyarov helped author the Advanced eBook Processor (AEBPR) software. This software allows Adobe eBook owners to translate their eBook software from Adobe’s secure format to Portable Document Format (PDF). However, one must own the eBook legally for the software to work. AEBPR has several beneficial uses. For example, the software has been used to convert eBook files into PDF files compati-

---

57 Id. § 512(h)(1).
58 Id. § 512(h)(2)(A).
59 Id. § 512(h)(2)(B)-(C).
60 Id. § 512(h)(3). The ISP is only required to disclose such information to the extent that it is available to them. Id.
62 See infra notes 79–82.
65 Id.; see Campaign for Digital Rights, supra note 63.
66 Free Dmitry Sklyarov!, supra note 64.
ble with electronic readers for the blind, and it has been used to move eBooks to different computers.

Although AEBPR software is legal in Russia, Adobe took issue with its use in the United States. On July 17, 2001, after presenting his program at a Las Vegas computer security conference, Sklyarov was arrested and charged with “distributing a product designed to circumvent copyright protection measures” in violation of the DMCA. After organizations such as the Electronic Frontier Foundation pressured Adobe, Adobe requested that the FBI drop the charges against Sklyarov and federal prosecutors backed off when Sklyarov agreed to testify against ElcomSoft. In the first criminal case tried under the DMCA, a jury acquitted ElcomSoft of all charges.

Another case DMCA opponents cite involves John Alex Halderman. Halderman, a Princeton University student, discovered that SunnComm Technologies’ CD-3 copy-protection software could be disabled by pressing the “shift” key while loading the CD into a computer. After posting a paper detailing his findings on his website, SunnComm threatened to sue under the DMCA. Ultimately, SunnComm relented on its threat to sue, though some observers be-

---

67 Id.; see Campaign for Digital Rights, supra note 63.
68 See Free Dmitry Sklyarov!, supra note 64. The author of this source suggests that this behavior is no different from someone creating a copy of a CD that he or she owns for use in his or her car. Id. It is important to note, however, that it could also be used to create copies for other individuals who did not purchase the product.
69 Campaign for Digital Rights, supra note 63.
70 Free Dmitry Sklyarov!, supra note 64. “As is usual practice for the computer security profession, his lecture was delivered from the perspective of exposing flaws in Adobe’s access-restriction technology.” Campaign for Digital Rights, supra note 63.
72 Campaign for Digital Rights, supra note 63.
74 Id. Jury foreman Dennis Strader later stated that the jury believed ElcomSoft’s software was illegal, but acquitted the company because they agreed the company had not intended to violate the law: “We didn’t understand why a million-dollar company would put on their Web page an illegal thing that would [ruin] their whole business if they were caught.” Id. (alteration in original). Strader also stated that the jury found the DMCA to be confusing, leading them to believe that Russian executives likely could not understand it. Id.
77 Dvorak, supra note 75.
lieve this was only because the case proved too "ridiculous" to pursue and would have reflected poorly on the DMCA.\textsuperscript{78}

Many critics also feel that the DMCA allows copyright owners to override fair use rights.\textsuperscript{79} Under traditional fair use doctrine, individuals are allowed to make incidental copies of copyrighted material without first obtaining the consent of the copyright owner.\textsuperscript{80} Some critics believe the fair use doctrine no longer applies in the electronic arena.\textsuperscript{81} For example, many CD manufacturers now use “copy-protected” CDs, which prevent even those who legally purchased a CD from making legitimate back-up copies of it.\textsuperscript{82} Additionally, the magazine \textit{2600}, a leading publication in the computer hacking community,\textsuperscript{83} was forbidden from placing a link on its website to another site

\textsuperscript{78} Id. Some critics of the DCMA wished that SunnComm had pressed charges against Halderman to bring attention to this "absurd law." Id. Indeed, comments SunnComm CEO Peter Jacobs made also support the argument that the case against Halderman was ridiculous:

Jacobs said in an interview . . . that a successful lawsuit would do little to reverse the damage done by the paper Halderman published . . . about his research, and any suit would likely hurt the research community by making computer scientists think twice about researching copy-protection technology. "I don’t want to be the guy that creates any kind of chilling effect on research," Jacobs said.

Fred "Zamboni" Locklear, \textit{SunnComm Shifts Stance, Backs Away From Lawsuit, Ars Technica}, Oct. 10, 2003, at http://arstechnica.com/news/posts/1065815462.html. An interesting point is that these comments appeared to directly conflict with ones Jacobs made the previous day, suggesting that Jacobs may have initially underestimated the possible effects of bringing suit:

This cat-and-mouse game that hackers and others like to play with owners of digital property is over. No matter what their credentials or rationale, it is wrong to use one’s knowledge and the cover of academia to facilitate piracy and theft of digital property. SunnComm is taking a stand here because we believe that those who own property, whether physical or digital, have the ultimate authority over how their property is used.


\textsuperscript{79} See 17 U.S.C. § 107 (1998) ("[T]he fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright.").


\textsuperscript{82} Id.

that displayed code that could be used to disable copy-protection software on DVDs. Some of these critics are worried that this pattern of behavior will ultimately lead to the demise of "free" information in places like public libraries.

Others argue that the DMCA "impedes competition and innovation" and serves as an "all-purpose ban on access to computer networks." Regardless of these criticisms, the DMCA appears to be here to stay. The Act has thus far withstood all constitutional challenges. Moreover, Congress supports the Act, though they have proposed minor changes to appease the DMCA's more strident critics. Additionally, a federal jury recently became the first to convict someone under the DMCA—a sign that at least a few are willing to enforce the Act. Nevertheless, while the public may appear willing to enforce the DMCA in certain situations, they seem less willing to do so in

---

84 See Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000). The disabling of the copy-protection software is necessary to play DVDs on a Linux-based operating system. See Boucher, supra note 80.

85 See, e.g., Boucher, supra note 80. A time may soon come when what is available for free on library shelves will only be available on a pay-per-use basis. It would be a simple matter for a copyright owner to impose a requirement that a small fee be paid each time a digital book or video documentary is accessed by a library patron. Even the student who wants even the most basic access to only a portion of the book to write a term paper would have to pay to avoid committing a crime.

86 Electronic Frontier Foundation, supra note 81. While it is important to briefly outline various criticisms of the DMCA in order to demonstrate its potentially rocky future, this Note focuses on private versus institutional enforcement of the DMCA. Thus, a more thorough probe of the criticisms of the DMCA is unnecessary, as its legal validity is a necessary presumption for purposes of this Note.

87 See, e.g., Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (holding that an injunction to prohibit the posting of DVD decryption software neither substantially oppressed more speech than necessary to further the government's interest nor unconstitutionally impinged on fair use rights); United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (finding that the DMCA is not overbroad, vague, nor an unconstitutional restriction of speech).


90 See Paul Festa, Jury Convicts Man in DMCA Case, CNET NEWS.COM, Sept. 23, 2003 (discussing the jury verdict against Thomas Michael Whitehead, who was convicted of selling hardware that could access DirecTV satellite broadcasts without paying for them. Three of the six felony counts he was convicted of were DMCA violations. He now faces up to thirty years in federal prison and fines of as much as $2.75 million), available at http://news.com.com/2100-1025_3-5080807.html.
others. Such inconsistency hardens attempts to enforce the Act, especially in the case of MP3 filesharing.

II
PRIVATE ENFORCEMENT OF THE DMCA

Private enforcement of the DMCA has not been easy. Much of the difficulty exists because society has tended to regard the behavior the DMCA criminalizes as acceptable. Although the thought of stealing a CD from a store is unacceptable, the act of file sharing, much like copying a CD at home, does not carry the same stigma. Moreover, the ease with which information may be shared over the Internet poses serious problems for enforcement of copyright laws such as the DMCA. Complicating matters further, advances in peer-to-peer technology have eliminated many intermediaries, such as ISPs, which has the effect of eroding the “gatekeeper” function intermediaries played in enforcing copyright laws.

A. Initial Strategy: Going After the Corporate “Big Guns”

At first, private entities, such as the RIAA, attempted to enforce the DMCA by going after companies that programmed or operated the peer-to-peer file sharing software used by millions to swap MP3 files. The first (and most popular) file sharing service the recording industry attacked was Napster. Although Napster was often referred to as a peer-to-peer service, it did not technically operate as such. Napster’s system was hierarchal in nature—all user searches passed between the user and Napster’s central server. In other words, when a Napster user ran a search, the search request would pass directly through Napster’s centralized servers, which in turn would inform the user of other users who had the file he desired. By contrast, with

---

91 See infra notes 269–73 and accompanying text.
93 See id.
95 Norman, supra note 22, at 373 (“[A]lthough no content is stored on, or passed through the central server, the centralized system arguably facilitates file sharing.”); see Part I.A.
96 See Norman, supra note 22, at 374.
98 See id.
99 See id.
true, or “pure,” peer-to-peer networks, all user queries are conducted between the individual users without the use of a central server.\footnote{Id.} Each user request independently searches the list of files that every other user is currently sharing on the network, and the software then pairs that user up with another from whom the requested file could be downloaded.\footnote{See id. (The query process and the list of results can look remarkably similar to Napster, and yet all of it can be accomplished without any reference to a central computer. Indeed, on true P2P networks, it is impossible to filter or block material from being swapped because there is no single place on the network to install a filter through which everything passes.)}

Napster distributed its file sharing software for free over the Internet via the company's website.\footnote{A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 901 (N.D. Cal. 2000).} The software allowed users to share MP3 files with other users logged-on to the server without paying each other, Napster, or the copyright owners.\footnote{Id. at 903. A sample taken by A & M’s expert revealed that eighty-seven percent of the sampled pieces were copyrighted. Id. Antipiracy counsel for the RIAA found that A & M owned copyrights to more than seventy percent of the files sampled. Id.} Although most of the music files transferred were copyrighted works, Napster never attempted to obtain authorization for such transfers from the owners of the copyrighted material.\footnote{Id. at 902. The company did have future plans to profit from the service. “Potential revenue sources include targeted email; advertising; commissions from links to commercial websites; and direct marketing of CDs, Napster products, and CD burners and rippers.” Id. In addition, Napster considered charging fees for premium versions of the software. Id.} Napster did not collect fees from its users, but the centralized peer-to-peer file sharing service was worth an estimated 60 to 80 million dollars.\footnote{Id. at 900.}

Various commercial recording corporations, including A & M Records, sued Napster alleging that its operation of a music file sharing service constituted contributory and vicarious copyright infringement.\footnote{See generally supra notes 79–81 and accompanying text (providing background on the fair use doctrine).} Napster defended by claiming that its users were making fair use of the copyrighted works.\footnote{Napster, 114 F. Supp. 2d at 904.} For example, Napster stated that users were using its service for “space-shifting,” or moving legally obtained content from one device to another, such as from a CD to a computer or MP3 player.\footnote{Id. at 912. This defense is also known as the “staple article of commerce doctrine.”} In addition, Napster used the affirmative defense of substantial noninfringing use.\footnote{Id.} The Napster Court noted that in Sony Corporation of America v. Universal City Studios, Inc., the Su-
The Supreme Court held that a “manufacturer is not liable for selling a ‘staple article of commerce’ that is ‘capable of commercially significant noninfringing uses.’” The Sony Court also observed that “[a]ny individual may reproduce a copyrighted work for a ‘fair use,’ the copyright owner does not possess the exclusive right to such a use.”

The District Court of the Northern District of California rejected all of Napster’s affirmative defenses and granted the plaintiffs’ motion for a preliminary injunction, which required Napster to shut down its service. The court analyzed Napster’s fair use argument under the four main factors codified in Section 107 of the Copyright Act and determined that Napster’s users were not engaging in fair use. The court also found that “space-shifting” only accounted for a “de minimis portion of Napster use.” Finally, the court refused to extend the Sony doctrine to Napster because Napster failed to show that space-shifting constituted a “commercially significant use of Napster.”

The court also held that the plaintiffs’ claims of contributory and vicarious liability were reasonably likely to succeed on the merits. The court found that Napster possessed actual knowledge that its users were illegally transferring copyrighted materials and that Napster materially contributed to the infringing activities. The court

---

110 Napster, 114 F. Supp. 2d at 912 (quoting Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 442 (1984)). The Seventh Circuit, however, has declined to follow the Ninth Circuit’s interpretation of the Sony doctrine, thus leading to the current split between the two circuits. See supra note 7.

111 Sony, 464 U.S. at 433.

112 Napster, 114 F. Supp. 2d at 896. The court found that there was a reasonable likelihood that the plaintiffs’ claim would succeed on the merits. Id.

113 17 U.S.C. § 107 (2002). The four factors are:

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

Id.


115 Id. at 904.

116 Id. at 916 ( [T]he most credible explanation for the exponential growth of traffic to the website is the vast array of free MP3 files offered by other users—not the ability of each individual to space-shift music she already owns. Thus, even if space-shifting is a fair use, it is not substantial enough to preclude liability under the staple article of commerce doctrine.

117 Id. at 918–22.

118 Id. at 918–19. The court held that this finding of actual knowledge precluded Napster from claiming relief under the safe harbor provisions of the DMCA, and that Napster failed to demonstrate that subsection 512(d) of the DMCA shelters contributory infringers. Id. at 919 n.24; see also 17 U.S.C. § 512(d)(1)(A), 512(d)(1)(B) (2000) (stating that the ISP must not have actual or constructive knowledge of infringing activity).

held that the plaintiffs would likely succeed on their vicarious liability challenge because Napster had "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."\textsuperscript{120}

The Ninth Circuit affirmed the district court, though the Court of Appeals remanded the case because its analysis was different in some regards.\textsuperscript{121} The Court of Appeals was unwilling to accept the lower court's holding that Napster's potential contributory and vicarious infringement liability precluded the application of the DMCA safe harbors.\textsuperscript{122} The Ninth Circuit did, however, state that the plaintiffs raised significant questions regarding the applicability of the safe harbor provisions, including:

(1) whether Napster is an Internet ISP [sic] as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give an ISP "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with § 512(i), which requires a ISP to timely establish a detailed copyright compliance policy.\textsuperscript{123}

Unfortunately, these questions were never answered because the lawsuit was automatically stayed when Napster filed for bankruptcy protection in June of 2002.\textsuperscript{124}

At first, this ruling appeared to be a major victory for the RIAA because it appeared that mass distribution of data was not possible without centralized file sharing services.\textsuperscript{125} This was, for a time, correct. Following the closing of Napster, many users flocked to the new "pure" peer-to-peer file sharing services.\textsuperscript{126} The result was an Internet "traffic jam."\textsuperscript{127} Without the aid of a central server, the individual users' computers were forced to process the search requests that were

\textsuperscript{120} \textit{Id.} at 920 (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996)). The court held that Napster can "police its service" since it possesses the ability to block users. \textit{Id.} at 920–21. The court also found that Napster would derive revenues "directly from increases in [its] userbase." \textit{Id.} at 921.

\textsuperscript{121} \textit{See} A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). The Ninth Circuit disagreed with some of the reasoning that the district court employed in its analysis of Napster’s contributory and vicarious liability. \textit{See id.} at 1019–24. However, the Court of Appeals ultimately affirmed the district court’s conclusion that the plaintiffs demonstrated a likelihood of success on the merits. \textit{Id.} at 1022–24. The Court of Appeals remanded for a modified preliminary injunction in accordance with its reasoning. \textit{Id.} at 1029. The modified injunction was subsequently affirmed on appeal. \textit{See A & M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1095 (9th Cir. 2002).}

\textsuperscript{122} \textit{Napster,} 239 F.3d at 1025.

\textsuperscript{123} \textit{Id.}


\textsuperscript{125} \textit{See} Borland, \textit{supra} note 33.

\textsuperscript{126} \textit{See id.}

\textsuperscript{127} \textit{See id.}
once handled by huge centralized servers. Thus, under the pure peer-to-peer services, "the network was only as strong—and as fast—as its weakest links."!

Over time, however, Internet connection speeds increased, thus making pure peer-to-peer services as efficient, if not more so, than their centralized predecessors. Copyright owners therefore had a new problem on their hands: a growing network of "pure" peer-to-peer file sharing services. Many recording companies, together with movie producing companies, sued some of these new services in an attempt to shut them down, as they had with Napster. The effectiveness of this approach is yet to be determined, as the circuits are currently split over whether liability should attach to these software creators for their users' infringing practices. The Supreme Court recently granted certiorari to resolve the dispute.

The two main cases exemplifying the opposing views are *Metro-Goldwyn-Mayer Studios, Inc. v. Groksster* in the Ninth Circuit and *In re Aimster Copyright Litigation* in the Seventh Circuit. In *Groksster*, the plaintiffs attempted to employ the same arguments they did in *Napster*. Although the Ninth Circuit did find that some users of the defendants' products were engaged in direct copyright infringement, the court affirmed the district court's summary judgment order for the defendants on both the contributory and vicarious liability claims. On the contributory infringement claim, the Ninth Circuit stated that while direct infringement is a requirement for contributory liability, it must also be established that the defendants had "knowledge of the infringement" and materially contributed to the infringement. To satisfy the knowledge requirement, the defendants must have had "reasonable knowledge of specific infringement." In other words, the defendants must have had "specific knowledge of

---

128 See id.
129 Id.
133 334 F.3d 643 (7th Cir. 2003).
134 See *Groksster*, 380 F.3d at 1160.
135 See id.
136 Id. at 1167.
137 Id. at 1160.
138 Id. at 1162. The Ninth Circuit found that this elevated standard applied because the defendants sufficiently demonstrated that their products were capable of "substantial noninfringing uses." Id. Thus, unlike in *Napster*, the *Sony* doctrine applied. See *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417 (1984). If the defendants failed to demonstrate this, the plaintiffs would only have needed to show that the defendants possessed
infringement at a time at which they contribute[d] to the infringement, and . . . fail[ed] to act upon that information."  

Unlike in Napster, the Ninth Circuit in Grokster determined that neither of the defendants materially contributed to the infringement. The Ninth Circuit distinguished the case from Napster, reasoning that the defendants in Grokster did not provide the "‘site and facilities’ for infringement" as the defendants in Napster had. Thus, the Ninth Circuit declined to hold the defendants liable for contributory infringement primarily because they operated on a more "pure" peer-to-peer format.

On the issue of vicarious infringement, the Ninth Circuit found that the defendants derived a financial benefit from the infringing conduct. But it ultimately determined that the defendants were not liable for vicarious infringement because they did not possess the right and ability to supervise the infringing conduct. As evidence of this, the Ninth Circuit cited the services' inability to prevent access by individual users, as well as their lack of centralized search indexes and mandatory registration systems—all of which Napster possessed. The defendants' failure to control its users, or to make the software such that its chances of being unlawfully used were minimized, were irrelevant in determining whether there is vicarious liability.

constructive knowledge of the infringement. Grokster, 380 F.3d at 1161. This interpretation of the Sony doctrine ultimately led to the split between the Seventh and Ninth Circuits.

140 Id. at 1163.
141 Id. ("Infringing messages or file indices do not reside on defendants' computers, nor do defendants have the ability to suspend user accounts." (quoting Grokster, 259 F. Supp. 2d at 1037, 1039–41)).
142 See id. (U)nder both StreamCast's decentralized, Gnutella-type network and Grokster's quasi-decentralized, supernode, Kazaa-type network, no central index is maintained. Indeed, at present, neither StreamCast nor Grokster maintains control over index files . . . . [E]ven if the Software Distributors "closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption." (quoting Grokster, 259 F. Supp. 2d at 1041)).
143 Id. at 1164. Both StreamCast and Grokster derived substantial revenue from advertising. "[B]ecause a substantial number of users download the software to acquire copyrighted material, a significant proportion of Defendants' advertising revenue depends upon the infringement." See Grokster, 259 F. Supp. 2d at 1044.
144 Grokster, 380 F.3d at 1164–66.
145 See id. at 1165; see also A & M Records v. Napster, 239 F.3d 1004, 1023 (9th Cir. 2001) (stating that the "ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise" the infringing conduct).
146 See Grokster, 380 F.3d at 1166 ("We agree with the district court that possibilities for upgrading software located on another person's computer are irrelevant to determining whether vicarious liability exists.").
Grokster appears to exonerate pure peer-to-peer software manufacturers of any secondary liability for actions committed by users with respect to copyright infringement. Indeed, the district court in Grokster acknowledged that it was “not blind to the possibility that [the] Defendants may have intentionally structured their businesses to avoid secondary liability for copyright infringement, while benefiting financially from the illicit draw of their wares.”147 As the Ninth Circuit later pointed out, however, “it is prudent for courts to exercise caution before restructuring liability theories for the purpose of addressing specific market abuses, despite their apparent present magnitude.”148 For the Ninth Circuit, resolution of this problem is best left to the legislature.149

Unlike the Ninth Circuit, the Seventh Circuit expressed a different view in In re Aimster Copyright Litigation.150 The facts of Aimster are similar to those in Grokster—owners of copyrighted music files brought suit against Aimster, a third-party program which was used to swap files through America Online’s Instant Messaging service.151 In Aimster, the dispute was whether the Aimster service utilized a Napster-like centralized database, as the plaintiffs claimed, or a more Grokster-like decentralized service, as the defendant asserted.152 The district court quickly brushed aside this distinction, which many had thought was central to these cases, stating that its reasoning in the case “would hold regardless of whether or not Aimster maintains a central database of files available for transfer.”153 The district court went on to grant the plaintiffs’ motion for preliminary injunction on the grounds that the plaintiffs “had demonstrated a likelihood of prevailing on the merits . . . with respect to vicarious as well as contributory infringement.”154 The injunction effectively shut down the Aimster service until the merits of the case were decided.155

On appeal, the Seventh Circuit affirmed the district court’s decision to enter the “broad” preliminary injunction against the defendant.156 Unlike the Ninth Circuit’s interpretation of the Sony doctrine in Napster and Grokster, the Seventh Circuit held that the mere capability of a product or service to have substantial noninfringing uses is

147 Grokster, 259 F. Supp. 2d at 1046.
148 Grokster, 380 F.3d at 1167.
149 See id.
150 In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), cert. denied, 540 U.S. 1107 (2004).
151 See id. at 645–46.
152 See In re Aimster Copyright Litig., 252 F. Supp. 2d 634, 641 n.6 (N.D. Ill. 2002), aff’d, 334 F.3d 643 (7th Cir. 2003), cert. denied, 540 U.S. 1107 (2004).
153 See id.
154 See Aimster, 334 F.3d at 646.
155 Id. at 645.
156 Id. at 656.
insufficient to defeat a claim of contributory infringement. According to the Seventh Circuit, in order to escape a claim of contributory infringement, the Sony doctrine requires not only a showing of possible substantial noninfringing use, but also a strong showing that the software is primarily used for noninfringing purposes. Noting that "Aimster has failed to produce any evidence that its service has ever been used for a noninfringing use, let alone evidence concerning the frequency of such cases," the Seventh Circuit swiftly affirmed the district court's order.

The Supreme Court recently granted certiorari in the Grokster case. If the Court adopts the Seventh Circuit's reasoning, the RIAA would possess a highly-effective tool to enforce its property rights under the DMCA. On the other hand, if the Court chooses to adopt the Ninth Circuit's interpretation, the RIAA may have to rethink its enforcement strategy, though it appears to have already begun a new enforcement approach.

B. A New Approach: Attacking Individual Users

To combat illegal file sharing, the RIAA has recently decided to sue individual users of pure peer-to-peer file sharing programs. Realizing that it could not go after every user of such software, the RIAA only subpoenaed heavy users who shared many files. These subpoenas were issued to prevent these users from further sharing files, while also instilling fear of prosecution in all other users.

The first wave of lawsuits came in September of 2003, when the RIAA filed suit against 261 individuals. The RIAA sued these individuals for as much as $150,000 per song that they allowed others to download from them. Although the RIAA stated that it would file thousands of additional lawsuits in the coming months, this did not

---

157 See id. at 653. "[W]hen a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitude of these uses is necessary for a finding of contributory infringement." Id. at 649.

158 See id. at 651, 653.

159 See id. at 653. The court was more hesitant with respect to the district court's ruling on the likelihood of success on the vicarious liability claim, but nevertheless affirmed the district court's ruling, largely because of its strong belief that the plaintiffs were very likely to prevail on the merits with respect to the contributory infringement claim. See id. at 654-55.


162 Id. The reason for such a high monetary amount is because of the tort remedies available under the DMCA. See 17 U.S.C. § 1203 (1999).

163 See Students Angry, supra note 161.
occur. In October of 2003, the RIAA filed eighty suits, and an additional forty-one suits in December of 2003, raising the total to 382. At least 220 of these suits settled for amounts ranging from $2,500 to $7,500 each. This pattern continued in January of 2004, when the RIAA brought four lawsuits that targeted 532 alleged infringers. It appears that this strategy of periodically filing lawsuits against small clusters of individuals will continue for the time being.

One way in which the RIAA sought to obtain the identity of alleged individual infringers was through use of the DMCA’s subpoena provisions. The strategyWithstood its first challenge in In re Verizon Internet Services, Inc., where the RIAA sought the identity of a Verizon Internet Service user who allegedly allowed others to download over 600 songs from his computer in one day. The RIAA served a subpoena upon Verizon under Section 512(h) of the DMCA to determine the identity of the user. Verizon refused to comply, claiming that the subpoena only “relate[d] to material transmitted over Verizon’s network, not stored on it, and thus [fell] outside the scope of the subpoena power authorized in the DMCA.” The RIAA countered by arguing that the subpoena power under the DMCA applies to all ISPs, regardless of “whether the infringing material is stored on or simply transmitted over the ISP’s network.”

The district court resolved the question in favor of the RIAA, ordering Verizon to disclose the identity of the alleged infringer. Following this victory, the RIAA served Verizon with another subpoena to disclose the identity of another individual allegedly sharing many copyrighted files. Once again, the district court held that this was a valid exercise of Section 512(h)’s subpoena power. Verizon appealed both of these orders and the D.C. Circuit reversed, reasoning that “a subpoena may be issued only to an ISP engaged in storing on

---

165 Id.
166 See id.
168 See 17 U.S.C. § 512(h); see also supra notes 57–60 (discussing the requirements of the subpoena provision).
170 See id. at 26.
171 See id.
172 Id.
173 Id.
174 Id. at 44–45.
175 In re Verizon Internet Serv., Inc., 257 F. Supp. 2d 244, 275 (D.D.C. 2003). The court also held that Section 512(h) does not violate Article III of the Constitution or the First Amendment. Id. at 248–68.
its servers material that is infringing or the subject of infringing activity."176 Thus, the Court of Appeals agreed with Verizon's initial contention that such subpoenas are only available against violators of Section 512(c) of the DMCA.177

It is uncertain how these recent rulings will affect the RIAA's newest strategy of suing individual users of file sharing programs. The Verizon case does not appear to be fatal to the RIAA's recent efforts, as it has continued to file lawsuits successfully against individual users.178 Additionally, there is evidence to suggest that the RIAA's strategy is being adopted even outside the United States. For example, Japanese police, in a rare 2003 crackdown, arrested two individuals for file sharing.179 Actions such as these suggest global cooperation in reducing online copyright violations. Nevertheless, the RIAA and similar organizations are hesitant to file large numbers of lawsuits because of the costs and negative publicity involved with suing individual infringers.180 Rather, these groups would prefer that the government assist the enforcement effort, both in detecting violations of and enforcing the DMCA. Thus far, it appears that the government is willing to offer such assistance.

III

FEDERAL INVOLVEMENT IN DMCA ENFORCEMENT

A proposed bill entitled the Piracy Deterrence and Education Act of 2003 would greatly increase the government's involvement in enforcing and detecting violations of the DMCA.181 This proposed bill operates under the premise that it is "important that Federal law enforcement agencies actively pursue criminals who steal the copyrighted works of others, and prevent such activity through

---

177 See id. at 1234–36.
178 See supra notes 166–68.
180 For example, a recent story alleged that the RIAA incorrectly filed suit against a seventy-nine year old man who then wrote a "handwritten note" to a federal judge explaining that he neither owns a computer nor knows how to operate one. See Students Angry, supra note 161. In addition, a recent survey indicates that two out of every three American teens, a major demographic for record sales, oppose fines for music file sharing. See Press Release, Harris Interactive, Two Out of Three American Teens Oppose Fines for Music File Shares, Says Harris Interactive Youth Survey (Oct. 9, 2003) [hereinafter Youth Survey], available at http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=683.
enforcement and awareness.”\textsuperscript{182} The most important provision of the bill directs the FBI to “develop a program to deter members of the public from committing acts of copyright infringement.”\textsuperscript{183} This program would require the FBI to monitor and detect individuals who are, without authorization, “offering on the Internet copies of copyrighted works, or . . . making copies of copyrighted works from the Internet.”\textsuperscript{184} The FBI would then have to “issu[e] appropriate warnings” indicating that such individuals “may be subject to criminal prosecution.”\textsuperscript{185} In addition, the FBI would be responsible for “facilitat[ing] the sharing among law enforcement agencies, Internet service providers, and copyright owners of information” regarding such activities.\textsuperscript{186} The Department of Justice would be required to employ agents who are “train[ed] in the investigation and enforcement of intellectual property crimes.”\textsuperscript{187}

The proposed bill also requires the Attorney General, in coordination with the Departments of Education and Commerce, to develop an Internet Use Education Program to educate the public on the value of copyrighted works and the ill effects of stealing such material.\textsuperscript{188} The program would inform the public of the “privacy, security, and other risks of using the Internet to obtain unauthorized copies of copyrighted works.”\textsuperscript{189} Finally, the bill requires the Attorney General to develop criteria under which copyright owners can use the FBI seal on physical and digital copies for deterrent purposes,\textsuperscript{190} an effort the FBI and RIAA began prior to this bill’s proposal.\textsuperscript{191}

Proponents of the bill, the RIAA being one of the largest, claim that such legislation will “strengthen the hand” of agencies such as the FBI to protect against online copyright infringement.\textsuperscript{192} The bill’s proponents emphasize the softer aspects of the proposal, such as the educational programs it would create and the use of the FBI seal on copyrighted products.\textsuperscript{193} Nevertheless, three significant problems emerge from the proposal.

\textsuperscript{182} \textit{Id.} § 2(7).
\textsuperscript{183} \textit{Id.} § 3(1).
\textsuperscript{184} \textit{Id.}
\textsuperscript{185} \textit{Id.} § 3.
\textsuperscript{186} \textit{Id.} § 3(2).
\textsuperscript{187} \textit{Id.} § 4.
\textsuperscript{188} \textit{Id.} § 5(b)(1).
\textsuperscript{189} \textit{Id.} § 5(b)(2).
\textsuperscript{190} \textit{Id.} § 7.
\textsuperscript{191} For example, the FBI and recording industry have been working at producing an FBI warning seal that can be used in the same way as it has been on videotapes, DVDs, and movies for years. \textit{See Hearing, supra} note 11.
\textsuperscript{193} \textit{See}, \textit{e.g.}, \textit{Hearing, supra} note 11 (describing why the FBI supports the Act).
First, the proposed legislation tends to "blur[ ] . . . distinctions between official prosecution of criminal acts and civil enforcement of copyright provisions." This bill would require the FBI to become more involved in private enforcement of the DMCA, while maintaining the façade that such participation is for criminal enforcement purposes. It permits the FBI to "scare a lot of users into thinking the government is after them." In other words, the FBI would, through the use of monitoring and issuing empty threats of criminal prosecution, privately enforce the DMCA in place of organizations such as the RIAA. Thus, the transaction costs of private enforcement of the DMCA would shift from organizations such as the RIAA to the government, and ultimately, taxpayers. Although private organizations like the RIAA would benefit from the use of the FBI's "scare power," government enforcement of the DMCA is an inappropriate use of public resources.

Second, the proposed legislation requires the FBI to facilitate information sharing between law enforcement agencies, ISPs, and copyright owners. Although it is clear that the RIAA and FBI would be more than willing to share information, the same might not be true for ISPs. Moreover, this may jeopardize privacy rights. For example, the FBI, or possibly even the RIAA, might require ISPs to divulge the personal information of its users whenever it wishes. The Verizon case suggests that ISPs will not have to disclose this information. In that case, however, the D.C. Circuit invalidated the use of subpoenas under the DMCA for user information only as a matter of statutory interpretation. Therefore, it would not be surprising for the same Circuit to enforce similar disclosure requirements under this proposed bill, as the language of the bill is much broader than that of the DMCA.

Third, the bill establishes a major policing responsibility for the FBI without providing clear guidelines explaining how the FBI is to execute this new responsibility. In fact, discussion regarding the pro-

---

194 Becker, supra note 192.
195 See id.
196 Id.
197 The Act only requires the FBI to issue "warnings to individuals . . . that they may be subject to criminal prosecution." Piracy Deterrence and Education Act of 2003, H.R. 2517, 108th Cong. § 3 (2003) (emphasis added).
198 See infra Part IV.
199 See H.R. 2517 § 3(2).
200 See Becker, supra note 192.
201 See Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1233 (D.C. Cir. 2003) ("[A] subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.").
202 See id.
program’s development is limited to one sentence. At no point does the bill ever address how the FBI is to identify potential violators; it only states that as part of the deterrence program, the FBI must issue warnings to violators. From this, one can conclude that the bill requires the FBI to monitor and detect potential violations of the DMCA. While some statutes are vague when assigning a task to a federal agency to allow some agency discretion in implementing the bill, the details of this proposed program should be more specifically articulated given the controversial nature of the broad, yet important task that this would impose on the FBI. In the absence of clear standards, the FBI might take the enforcement regime too far, or simply not answer the call in the first place.

The Piracy Deterrence and Education Act is not the first piece of controversial legislation Representative Howard Berman has proposed that is designed to curb online music piracy. In 2002, Representative Berman proposed legislation (the Berman Bill) to amend the U.S. Copyright Law to relievecopyrighters of liability for “disabling, interfering with, blocking, diverting, or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work on a publicly accessible peer-to-peer file trading network.” The only limitation was that such impairment could not “without authorization, alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader.”

Under the Berman Bill, a copyright owner could cause damage of up to $50 to an infringer’s computer (not including damage to files containing the copyrighted material). For a victim to bring a claim for wrongful impairment, however, she would have to demonstrate that she suffered an economic loss in excess of $250. In addition, a user would need to show that the copyright owner “knowingly and intentionally” impaired him without having a “reasonable basis” to believe that the user was conducting infringing conduct. The Berman Bill may have had good intentions in granting copyright owners technological power to protect their works, but the bill failed to afford sufficient protection to innocent victims. This criticism applies equally to the Piracy Deterrence and Education Act of 2003. The

203 See H.R. 2517 § 3(1).
204 See id.
205 Id. § 3.
206 H.R. 5211, 107th Cong. § 1(a) (2d Sess. 2002).
207 Id.
208 Id. § 1(b)(1)(C).
209 Id. § 1(d).
210 Id.
211 See Norman, supra note 22, at 399–400.
Berman Bill eventually died in committee—the same committee now considering the Piracy Deterrence and Education Act. Hopefully Berman’s second attempt will suffer the same fate.

IV

WHY INCREASED INSTITUTIONAL INVOLVEMENT IN DMCA ENFORCEMENT IS UNNECESSARY AND ALTERNATIVES FOR REQUIRED EFFECTIVE PRIVATE ENFORCEMENT

Despite the contentions of organizations such as the RIAA, enforcement of Internet copyright regulations is better left to the private sector. The DMCA was enacted to “restore an eroding gatekeeper system,” which once permitted copyright owners to independently police the few intermediaries who could access their work. The DMCA provides private actors with a more than sufficient means of enforcing their copyrights.

First, the DMCA may provide the means by which the RIAA can simply shut down any file sharing service where unauthorized sharing of copyrighted files takes place. This strategy proved effective with Napster and may, depending on how the Supreme Court rules, hold true with the more modern pure peer-to-peer software. While there may be no true way to effectively shut down these pure peer-to-peer programs, if organizations such as the RIAA are able to bring contributory and vicarious copyright infringement suits against the manufacturers of such software, other manufacturers would likely be deterred from producing such software in the future.

Regardless, the high reputational and transactional costs that the RIAA and similar organizations incur through private enforcement against individuals do not justify government intervention. Occasionally, the RIAA must assume the “bad guy” role in the effort to run its business effectively, and playing this role requires it to weigh the costs and benefits behind the decision to pursue copyright infringers. This calculus is similar to that made by retailers who must choose between protecting their product from theft and maintaining a positive public image. One aspect of that calculus is setting acceptable loss rates.

The government does not monitor individuals while they are at retail outlets to prevent shoplifting. In such circumstances, the re-

---

212 Wu, supra note 92, at 741.
213 See A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); supra Part II.A.
214 See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004), cert. granted, 125 S. Ct. 686 (2004); supra notes 131–61 and accompanying text.
215 Norman, supra note 22, at 392 (“Copyright owners have long avoided suing direct infringers for file-sharing due to obvious concerns: the cost and the negative publicity associated with filing multiple lawsuits against individual users would be overwhelming.”).
responsibility to supervise the actions of customers rests with the individual outlet. If the store catches someone shoplifting, the store decides how to handle the situation. The store may report the shoplifter to the authorities if it so chooses, or it may privately reprimand the shoplifter. It is the store’s responsibility to protect its own property, though it ultimately has the support and aid of the criminal justice system. Why should the government assume the active role of the protector simply because the offense occurs online?216

Copyright infringement via peer-to-peer services is a new problem. It will likely take time for entities like the RIAA to develop effective control strategies. Although the DMCA was just the first step in granting private entities the independent power to protect their copyrights online, it was a major one. It is true that the RIAA has had difficulties with enforcing the DMCA while maintaining a positive public image.217 These tribulations, however, result from the RIAA’s inexperience in the area. Over time, the RIAA will be able to correct these deficiencies and strike a balance similar to that done by ordinary retail outlets seeking to protect their products.

Regardless of the difficulties faced by the RIAA in enforcing the DMCA, it is clear that increased governmental involvement is not the answer. That is not to say that some involvement is not acceptable. For example, the RIAA should be able to use the FBI seal as a tool to frighten potential infringers. But small involvement like this can and will occur without legislators consuming excessive public resources—in fact, it already has.218 All that proposed bills like the Piracy Deterrence and Education Act of 2003 do is remove the burden of privately enforcing the DMCA from copyright holders and place the burden on the government, and ultimately the public. Such shifting of responsibilities wastes taxpayer resources.219

---

216 The two situations are admittedly different. For example, a store-level decision to prosecute an individual shoplifter would not have the same nationwide implications as active FBI involvement in prosecuting thousands of individual downloaders across the United States. Nonetheless, the analogy illustrates the principle that similar conduct (catching a shoplifter stealing a CD from a store or catching an individual illegally downloading a song from the Internet) should not be treated differently.

217 See, e.g., Students Angry, supra note 161 (describing a seventy-nine year old man who was sued by the RIAA for violating the DMCA despite the fact that the elderly man claims he does not even own a computer or knows how to operate one); Youth Survey, supra note 180 (citing a study finding that two-thirds of American teens oppose the fines for file sharing sought by the RIAA).

218 See Hearing, supra note 11.

219 The decision of the Ninth Circuit in A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001), supports RIAA’s active role. In Napster, the court stated: “[W]e place the burden on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content.” Id.
In terms of criminal sanctions, the DMCA imposes stiffer penalties than one sees for ordinary shoplifting. For example, a first-time offender caught illegally downloading a single copyrighted song could be subject to a $500,000 fine or five years imprisonment. Repeat offenders could receive a $1,000,000 fine or ten years imprisonment. Shoplifters caught stealing a CD from a retail store would not face such serious sanctions, and would receive nothing more than a slap on the wrist. In New York, for example, one who shoplifts a CD would face petty larceny charges or criminal possession of stolen property in the fifth degree. Both are class A misdemeanors and carry a maximum fine of $1,000 or imprisonment of up to one year. This is a substantial difference compared to the possible criminal sanctions for violating the DMCA, even though a CD contains many songs, while a DMCA violation can result from downloading or sharing only one copyrighted song.

The stiffer criminal sanctions under the DMCA help compensate for “the ease with which copyright works can be copied [online] and the scale on which it can be done.” But the DMCA does not stop with criminal sanctions. It also provides another key form of relief to copyright holders: the right to file a civil action. Under the DMCA, any person injured as a result of a DMCA violation may bring a civil action against the infringer. When faced with such an action, the court may issue a temporary or permanent injunction, order the “modification or the destruction of any device or product involved in the violation,” or award damages.

The key component of these civil actions is the right to receive damages. Any damages awarded under these provisions are independent of possible criminal fines. The damages provisions have both a compensatory and punitive element, though the statute does not use such terms. The DMCA’s damages provisions permit an injured party to collect the actual damages sustained, plus any additional profits

---

220 Cf. David I. Bainbridge, Introduction to Computer Law 380 (4th ed. 2000) (“The scope and magnitude of criminal penalties have been gradually increased and strengthened to cater for the growing ease of copying with the advent of high speed . . . computers.”).
222 See id. § 1204(a)(2).
224 See id.
225 See id. §§ 70.15(1), 80.05(1).
226 Bainbridge, supra note 220, at 330.
228 Id. § 1203(b)(1); see A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 901 (N.D. Cal. 2000), reversed in part, 239 F.3d 1004 (9th Cir. 2001) (granting injunctive relief to injured plaintiffs).
230 See id. § 1203(b)(3).
made by the violator that are attributable to the infringing conduct.\textsuperscript{231} This recovery of profits plays the role of the compensatory element of the damages provisions.

Alternatively, the injured party may elect to receive statutory damages.\textsuperscript{232} If an injured party elects this option, he would instead receive an award between $200 to $2,500 for each violation of Section 1201 of the DMCA,\textsuperscript{233} and $2,500 to $25,000 for each violation of Section 1202 of the DMCA.\textsuperscript{234} This section represents de facto punitive damages, since the possible amount of the award far exceeds any actual loss sustained by the injured party.\textsuperscript{235}

Some skeptics may argue that the amount of statutory damages is not excessive since the probability that a song would only be downloaded once is minimal. Nevertheless, the amount of statutory damages listed in the statute is for \textit{each} violation. In other words, the DMCA arguably gives an injured party the right to statutory damages for each time a file is downloaded illegally.\textsuperscript{236} Thus, the increase in actual losses sustained by the copyright holder would be proportional to the increase in available statutory damages under the DMCA.\textsuperscript{237}

These high statutory, or punitive, damages make the DMCA a highly-effective tool for private entities to protect their copyrights online. The drafters of the DMCA made it very easy for copyright holders to obtain these statutory damages during the course of a civil action, and can be elected any time prior to the final judgment being entered.\textsuperscript{238} These damage amounts are much higher and easier to obtain than those available to ordinary retail outlets.\textsuperscript{239} A store, or the record company for that matter, is not statutorily entitled to receive thousands of dollars from someone for shoplifting a CD (with multi-

\textsuperscript{231} See id. § 1203(c)(1)(A).
\textsuperscript{232} See id. § 1203(c)(1)(B).
\textsuperscript{233} See id. § 1203(c)(3)(A). Section 1201 of the DMCA refers to circumvention of copyright protection systems. See id. § 1201(a)–(b); supra notes 40–43 and accompanying text.
\textsuperscript{234} See id. § 1203(c)(3)(B). Section 1202 of the DMCA refers to the integrity of copyright management information. See id. § 1202(a)–(b).
\textsuperscript{235} For example, each time a party illegally shares an MP3 song file, the most that the copyright holder could claim in actual losses is the price of the CD that the song is on.
\textsuperscript{236} See 17 U.S.C. § 1203(c)(3)(A), (B).
\textsuperscript{237} For example, suppose the price of a CD is $10. If a song was shared only once, the copyright holder (likely the record company) would only suffer, at most, $10 in actual damages. However, the copyright holder would possibly be able to receive up to $25,000 in statutory damages, netting him a gain of $24,990. Now, assume the song was shared twice. The actual losses would be, at most, $20. However, the record company could potentially receive up to $50,000 in statutory damages for the two violations of the DMCA. This would give the record company a net gain of $49,980. It is important to note that this presupposes that the individual being charged is capable of paying such high damages without becoming insolvent. Obviously, the higher the amount gets, it is less likely to be the case that one could pay the damages without becoming insolvent.
\textsuperscript{238} See 17 U.S.C. § 1203(c)(3)(A), (B).
\textsuperscript{239} See supra notes 232–35 and accompanying text.
ple songs). The store would be fortunate to retrieve the stolen CD or receive its cash value.

As one commentator has pointed out, "[T]ort remedies will have the potential to fill the enforcement gap in cyberspace, especially where law enforcement agencies have not addressed high-tech issues." Because tort remedies fill the enforcement gap, law enforcement agencies do not need to become involved in the enforcement process. Copyright holders should be able to notify the authorities of a DMCA violation if they feel criminal sanctions are appropriate for the violator, much like the practice of retail outlets today.

Even if other circuits follow the D.C. Circuit's reasoning in Verizon, with the effect of possibly making identification of individual online infringers more difficult, this does not mean that government involvement is necessary. The high-damage awards mean that even small numbers of enforcement actions will likely result in high levels of deterrence. Moreover, although it may be more difficult to detect infringers and obtain judgments against them, the copyright holder has a substantial monetary incentive to pursue the private enforcement option.

Furthermore, copyrighters should implement measures to make their products more difficult to steal online. The primary responsibility for protecting a product must fall on its owner. If the techniques used by retailers to prevent shoplifting were not perfected over time, then intuitively there would be higher levels of theft. Although

240 Rustad, supra note 94, at 66.

Tort remedies are more flexible than criminal law and can be updated more easily to adapt to cyberspace. Tort law carries no death penalty and cannot incarcerate a defendant. Instead, it offers the remedy of punitive damages—civil punishment in the form of monetary damages proportional to the wealth of the defendant. Tort remedies adapted to Internet wrongdoing will play an increasingly important role in punishing and deterring fraud, hacking, and other wrongdoing on the Internet.

Id. 241 See id. at 115 (arguing that legal time lags makes criminal statutes quickly outdated in the area of "cybercrime enforcement," creating an "impossible burden to meet at a time when emerging technologies give rise to novel forms of socially harmful behavior").

242 Additionally, copyright holders may wish to notify the authorities if they plan on collecting heavy tort damages from an individual, as such documentation will only strengthen their case against the individual.

243 See Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1233 (D.C. Cir. 2003) (holding that "a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity").

244 The legislature could simply overturn this decision by amending the DMCA so as to require ISPs to disclose user information, even if the illegally transferred files are not stored on their servers.

245 See Rustad, supra note 94, at 66.

246 See Patricia-Anne Tom, Security: Stopping the Shrink, RETAIL TRAFFIC (Apr. 1, 2000) (noting that store owners have a responsibility in the fight against shoplifting and explain-
"digital technology facilitates the copying and distribution of digital information, it also permits greater control over the use and distribution of information." Thus, as technology further develops, "authors and publishers can have more, not less, control over their work." Since digital technology needs computer code to operate, "computer code can be used to regulate behavior."

The RIAA could use computer code to strengthen the anticircumvention technology on CDs, thus making them harder to "rip" into MP3 files. In this vein, the RIAA has taken limited steps to curb the spread of MP3s, including the proposal of the Secure Digital Music Initiative (SDMI). If adopted, the SDMI would require consumer electronics manufacturers to adopt trusted systems technology before commercially recorded music could be played on their components. If effective, this program could prevent CDs from being ripped, copied, burned, or downloaded for free. Efforts like these are preferable to increased government intervention and surveillance of individual online activity.

Patience truly is a virtue when dealing with this new problem. Current attempts at private enforcement of the DMCA have proven effective at deterring illegal MP3 file sharing without excessive government intervention. Just the threat of legal action prompted many

---

248 Id. (quoting Mark Stefik, _Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing_, 12 BERKELEY TECH. L.J. 137, 138 (1997)).
249 Id. (citing LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999)).
250 See id. at 275–76.
252 "Trusted systems use encryption to prevent unauthorized access to digital content, and they use rights management to determine what 'rights' any given user has with respect to that content." Id. at 274–75 (footnotes omitted). Thus, "through the use of trusted systems, current copyright holders can use technology to control how works are accessed." Id. at 274.
253 Id. at 275.
254 Id. at 276. The RIAA can look at what has been done with DVDs:

The motion picture industry adopted a similar approach with digital movies distributed on DVDs. Each DVD is encrypted by a copy protection system known as the Content Scramble System ("CSS"). A movie recorded on DVD may only be viewed on players and computer equipment using CSS-licensed technology, and the equipment is programmed to permit the user to play, but not copy, the movie.

_Id._ (footnotes omitted).
individuals to delete all MP3s from their computer.\footnote{For instance, after the RIAA launched its aggressive campaign against individual MP3 file sharers in May of 2003, 606,000 households deleted all MP3 files on their computers. This rate continued to increase, with 1.4 million households deleting all MP3 files in August of 2003. In addition, there has been a decrease in overall MP3 file sharing via peer-to-peer networks. In April of 2003, 852 million MP3 files were traded. By June of 2003, this number fell to 655 million. From August to September of 2003, the total number of households acquiring MP3 files via peer-to-peer networks declined by eleven percent, and the total number of MP3 files downloaded decreased by nine percent. These figures indicate that the mere threat of private enforcement has proven effective at protecting the interests of the RIAA and other copyright holders by deterring individuals from sharing and downloading MP3 files. Once actual civil and criminal judgments are obtained against some individuals, these numbers are likely to continue their trend at an even more rapid pace.}

There are also nontechnological measures the RIAA can implement to limit illegal file sharing. For example, the RIAA could work at changing the public perception of both the record industry as a whole and the severity of the effects of file sharing on the industry and its artists. The RIAA has made an attempt at this. Its website now has an area dedicated to informing the public about what constitutes piracy, its negative effects, and recent news on the battle against it. Another organization, Music United for Strong Internet Copyright ("MUSIC"), has also launched a campaign against piracy. This or-

\footnote{According to The NPD Group (Aug. 21, 2003), at http://www.businesswire.com/webbox/bw/082103/232335023.htm.}

\footnote{See Press Release, supra note 255.}

\footnote{See id.; Business Wire, supra note 255.}

\footnote{See Press Release, supra note 255.}

\footnote{See id.; Business Wire, supra note 255.}

\footnote{See Business Wire, supra note 255.}

\footnote{See id.}

\footnote{See Press Release, supra note 255.}

\footnote{An effective enforcement mechanism is one of the three fundamental characteristics of enforceability. See Christopher Reed, Internet Law: Text and Materials 266–67 (2000). The others are: (1) "that compliance with the law or regulation [is] . . . feasible," and (2) that the law is "limited in its application to those over whom the legislator has a legitimate claim." \textit{Id.} at 266. The other two criteria mentioned above are satisfied as well. With respect to the first characteristic, compliance with the DMCA is certainly feasible: all one has to do is cease downloading copyrighted music without permission. With respect to the second characteristic, the DMCA only applies to individuals within the jurisdiction of the United States.}


ganization uses celebrities to spread its antipiracy message.\textsuperscript{266} One author suggests that "educational campaigns should rely less on famous artists and large organizations to spread the antipiracy message and more on the impact file sharing has on lesser known artists, songwriters and independent labels."\textsuperscript{267} This approach may be problematic, however, because some artists actually benefit from the widespread sharing of their songs. Widespread swapping of an unknown artist's song can occasionally open the door to superstardom for these individuals. For example, singer John Mayer attributes much of his newfound success to file sharing: "Napster has come and gone, and a lot of people think it didn't do all that much for anybody... But it bolstered the careers of a few people, and I was one of them."\textsuperscript{268}

The RIAA should also make a stronger attempt to alter the public perception of file sharing. People understand that stealing a CD from a store is wrong. Yet a recent poll revealed that two-thirds of American teens oppose fines for file sharing.\textsuperscript{269} The study found that nearly eight out of ten American teens feel that sharing and downloading copyrighted music files should be legal.\textsuperscript{270} Another study found that seventy-eight percent of the people who download music do not feel that they are stealing—fifty-three percent of general Internet users agreed with them.\textsuperscript{271} Sixty-one percent of those who download music claimed that they could care less if the music is copyrighted.\textsuperscript{272} Yet another study concluded that there is a public norm that copying for others is acceptable, so long as it is not for profit.\textsuperscript{273} The RIAA needs to work at changing this perception so that illegal file sharing is viewed as being as immoral as shoplifting. If the RIAA can convince society that this behavior is unacceptable, enforcement of the DMCA


\textsuperscript{267} Norman, \textit{supra} note 22, at 405.


\textsuperscript{269} May\'er's newfound assurance carries over to his fans, whom he encourages to tape his performances. It's not unusual for a gaggle of wire-strewn squares to arrive long before showtime, set up microphone stands and, within minutes of returning home, upload the concerts on the Internet, where a thriving John Mayer file-sharing community exists.

\textit{Id.}

\textsuperscript{270} See Youth Survey, \textit{supra} note 180.


\textsuperscript{272} \textit{Id.}

would be a much easier task—in fact, it would likely lead to a decrease in DMCA violations.\textsuperscript{274}

Additionally, the RIAA should also work at changing the “us versus them” mentality that many consumers have. One way that this can be accomplished is by lowering the prices of CDs. This will help change the public perception that the record companies are charging exorbitant prices, which may not be an erroneous belief. In September of 2002, five U.S. record distributors settled a lawsuit brought by forty-one states for $143 million dollars.\textsuperscript{275} The lawsuit claimed that these distributors were involved in an illegal price-fixing scheme to keep CD prices high.\textsuperscript{276} If the record industry worked at making CDs more affordable,\textsuperscript{277} individuals may feel worse about illegally downloading MP3 files.

\section*{Conclusion}

The illegal distribution of copyrighted music files is a recent but pervasive problem. The recording industry will do everything in its power to protect its assets, including asking the government to do it for them. Congress, eager to aid in the process, passed the DMCA to help private entities protect their copyrights online. This legislation has enabled private entities to receive high punitive awards from online infringers. Additionally, the DMCA carries with it the threat of stiff criminal sanctions. The RIAA has utilized the DMCA to attack both the providers of file sharing services, and, more recently, the individual users of these services. Despite the effectiveness of these attacks, the RIAA has become impatient and maintains that it needs strong government involvement in the process.

\textsuperscript{274} See Wu, supra note 92, at 723 (describing how “statistics suggest that P2P applications have . . . successfully sidestepped social norms that might otherwise bolster compliance with the copyright regime”).

\textsuperscript{275} See Norman, supra note 22, at 405–06.

\textsuperscript{276} See id. at 406.

\textsuperscript{277} This could be done not only by lowering the prices of CDs, but also by making the songs available for download online at a discounted price. Since many people are willing to download songs online, it follows that many are not concerned with glitz, unnecessary packaging that accompanies store-bought CDs. Thus, by cutting costs, the record industry could drive down CD prices. Alternatively, the record industry could build value into the “extras” that come with the CD. If people believe that they are actually getting something of value when they purchase the CD, they may be more apt to actually do so. See id. at 408–09 (suggesting packaging methods the record industry could use to build value in the store-bought product); see also Bill DeMain, John Mayer Inside Looking In, PERF. SONGWRITER, Mar.–Apr. 2003, at 45, 49–50 (What we’re up against right now, in terms of music industry, in terms of file sharing, in terms of losses, is not a matter of “How do we tell kids to stop stealing?” Because it’s not stealing. It’s a matter of “How do we turn people on to the experience of owning a CD?” (quoting musician John Mayer)).
The government has strongly supported the RIAA in its battle. Copyrighters can use the FBI seal on digital recordings and the RIAA can avail itself of the stiff DMCA-created civil and criminal penalties. Further legislation mandating even further government involvement, however, is unnecessary. Proposed legislation like the Piracy Deterrence and Education Act of 2003 unfairly shifts the burden of enforcing the DMCA on the government, and ultimately, on the taxpayers. In addition, this proposed legislation is too overbearing and vague—especially in light of the substantial powers it grants.

Instead of lobbying for legislation that increases government involvement in DMCA enforcement, the RIAA should focus on other means to correct the problem. Digital technology has “the power to set music free,” but it can also “lock it up.”278 Through enhancing anticircumvention technology, the RIAA can prevent the creation of unauthorized MP3 files. Additionally, the RIAA should work at altering the public’s perception of both the recording industry and of unapproved file sharing of copyrighted works. Through these efforts, the RIAA can protect their assets without wasting government resources, thus permitting such resources to be better allocated to serving society’s needs.

278 Ku, supra note 247, at 276.