PIRACY DESERVES NO PRIVACY

Frank Chao[1]
Duke University School of Law
Frank.Chao@law.duke.edu.

The Recording Industry Association of America ("RIAA"), the music industry's trade and lobbying group, recently initiated a controversial tactic to bring to surface previously anonymous digital pirates of the Internet. This aggressive tactic aims to make safe the digital oceans for copyright and involves identifying and bringing claims against infringing individuals who download, swap, and/or post copyrighted music illegally via the Internet. The RIAA cares not who the infringers are or whether the infringers know the illegality of their actions. Nor does the music industry concern itself with the inevitable storm of backlash bound to fall upon them for suing uninformed or unintentional infringers. Internet users and privacy advocates, however, care all too much. This i-brief attempts to alleviate the fears of privacy infringement by bringing to light certain safeguards built into the Digital Millennium Copyrights Act ("DMCA") to deal with the possibility of both fraudulent identity subpoenas and infringement into personal privacy. In addition, case law will show that the subpoena powers of the DMCA will not be abused by those who truly wish to enforce copyright laws and legitimate claims of ownership, thereby maintaining the privacy of law abiding Internet users.

MUSIC INDUSTRY FILES SUITS AGAINST INDIVIDUAL INFRINGERS

¶1 On September 9, 2003, the New York Daily News reported that the Recording Industry Association of America ("RIAA") brought suit against Brianna LaHara, a twelve-year-old Catholic school honor student residing in Manhattan.[2] Brianna utilized Kazaa[3] to download numerous copyrighted songs. Brianna's mother, Sylvia Torres, eventually settled with the RIAA for $2000.00. As a single mother, Sylvia should certainly feel that her honor student daughter now knows more about copyright than before. Although the lesson in copyright law should not have cost $2000.00, the RIAA hopes that its heavy-handed methods and teachings will strike fear into the pirating community. Similar cases and suits involving unsuspecting, as well as intentional, digital pirates are being reported throughout the nation. The reason for so many lawsuits stems from the tremendous number of illegal downloads taking place. The technology acting as a conduit for illegal downloading is provided by the various Peer-to-Peer ("P2P") programs available to would-be pirates. The company responsible for creating KaZaa stated that 230 million copies of KaZaa have been downloaded for

---

[1] Mr. Frank Chao attends the Duke University School of Law in Durham, North Carolina. He will graduate in May of 2004 with a J.D. and LL.M. in International Law.

[2] Frank Ahrens, *RIAA's Lawsuits Meet Surprised Targets Single Mother in Calif., 12-Year-Old Girl in N.Y. Among Defendants*, Wash. Post, Sept. 10, 2003, at E1, *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A51698-2003Sep9&notFound=true.

[3] KaZaa is a Peer-to-Peer ("P2P") software application allowing users on its network to exchange computer files with each other.

free.[4] Given the recent and excessive damage already sustained by the music industry, the RIAA must now implement a final option: individualized enforcement of copyrights. Other options, including sitting idly as pirates usurp copyrighted music and adopting educational campaigns (to convince people that paying for music is somehow better than acquiring music free of charge), do not seem to be working very well. Given that neither inaction nor education seem to deter Internet users from illegally downloading copyrighted music, the RIAA has been tracking numerous pirates and filing suits against them.

CONDUITS TO THE INTERNET

¶2 The RIAA has taken control of enforcing copyright laws because no other party or person is doing so. In fact, certain parties not only provide conduits for the pirates into the digital realm, but they also delay potential copyright enforcement claims by shielding the pirates from judicial sight and grasp. The main conduits include college campuses and Internet Service Providers ("ISPs"). In one month alone, the RIAA filed 871 subpoenas in United States District Court in Washington D.C., demanding that universities and ISPs provide the RIAA with personal information about the users of PSP networks, such as KaZaa.[5]

Universities

¶3 Because of the academic need for extensive high speed Internet connection on campuses, college institutions inadvertently foster widespread P2P file-sharing and downloading of copyrighted music, movies, video games and software off the Internet. College campuses have been targets of RIAA and music industry subpoenas demanding the identities of the infringers the RIAA plans to sue.[6] Some colleges have delayed the enforcement measures of the DMCA by claiming procedural violations. Boston College and Massachusetts Institute of Technology ("MIT") filed motions to quash the subpoenas filled by the RIAA, arguing that the subpoenas were served in Boston, more than 100 miles away from where they were filed in federal court in Washington, D.C.[7] Boston College and MIT opposed the subpoenas based on Federal Rules of Civil Procedure which states in pertinent part, "a subpoena may be served at any place within the district of the court by which it is issued, or at any place without the district that is within 100 miles of the place . . . specified in the subpoena . . . ."[8] Although colleges and universities have an interest in protecting the private information of their students and faculty, these institutions should also take measures to prevent piracy on

---

[4] Br. of Amici Curiae Motion Picture Ass'n of Am., Inc. et al. at 8, In re Verizon, Nos. 03-7015, 03-7053 (consolidated appeals) (filed 2003).
[5] Matt Hines & John Borland, *Schools Stay Mum on File Trader's Names*, CNET NEWS.COM, *at* http://news.com.com/2100-1027_3-5052884.html (last modified July 22, 2003).
[6] Lesli A. Maxwell, *Colleges Aim to End Piracy, Guard Privacy*, THE SACRAMENTO BEE, Aug. 18, 2003, *available at* http://www.sacbee.com/content/news/education/story/7248099p-8193210c.html.
[7] James Collins, *BC, MIT Decline to Name Students in Music-use Case*, THE BOSTON GLOBE, July 22, 2003, *available at* http://www.boston.com/news/daily/22/mit_bc.htm.
[8] Fed. R. Civ. P. 45(b)(2) (2001).

their computer networks because of their own reliance on copyright laws to protect their academic products.[9] For example, colleges retain copyright ownership in works produced by individuals as part of the employee's job. These works include computer software developed by a staff member from Computing Services, articles written for alumni and faculty magazines, or other publications written by the Office of Publications.

Internet Service Providers

¶4 Another critical source of Internet connection allowing copyright infringement include ISPs. The RIAA has targeted the greater part of the subpoenas towards private ISPs, such as Comcast and Verizon Communications ("Verizon"), whose patrons download copyrighted material through their home personal computers. At the end of 2002, RIAA demanded that Verizon identify one of its customers accused of swapping music files and violating copyright laws. Following a challenge by Verizon, District Judge Bates ordered Verizon to release the identity of the Verizon customer suspected of pirating copyrighted music.[10] The importance of the Verizon case lies in its status as a test case for the DMCA subpoena power, a power affirmed by the District Court, which allows music companies to require ISPs to release the names of their customers suspected of violating copyright laws.[11] Verizon appealed the decision, but the holding should be affirmed because copyright laws clearly state that copyright owners have a right to obtain the identity of the infringer for the purposes of enforcing copyright protection.[12]

COPYRIGHT LAW

¶5 An underlying purpose of copyright law, as with other forms of intellectual property law, is to support artistic endeavors by allowing artists to benefit from their creations.[13] The justification for providing a "special reward" (monetary incentives) for artists and creators to continue to create lies in the enrichment of public well-being through the sharing and enjoyment of the "products of their genius . . . ."[14] The ultimate source of copyright law stems from the Constitution and flows through the legislature: "The Congress shall have Power . . . To promote the Progress of Science and the useful Arts, by securing for limited times to Authors and Inventors the Exclusive Right to their respective Writings and Discoveries."[15] Congress has

---

[9] Maxwell, *supra* note 6.
[10] In re Verizon, 240 F. Supp. 2d 24, 45 (D.D.C. 2003).
[11] *Id*.
[12] 17 U.S.C. § 512(h)(1) (2002) ("[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 . . . .").
[13] Greg Adams, *A Proposal for Rebalancing the Digital Partnership Between Content Providers and Internet Gate-Keepers*, 13 DEPAUL-LCA J. ART & ENT. L. & POL'Y 203, 204 (2003); *see, e.g.*, Eldred v. Ashcroft, 123 S. Ct. 769 (2003) (quoting Mazer v. Stein, 347 U.S. 201, 219 (1954)), Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, (1985) (quoting *Mazer*, 347 U.S. at 219), Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984), *Mazer*, 347 U.S. at 219.
[14] Sony, 464 U.S. at 429.
[15] U.S. Const. art. I, § 8, cl. 8.

subsequently created and instituted various other forms of copyright law, such as the Copyright Act of 1976.[16] The Copyright Act laid out the five exclusive bundles of rights for authors: (1) reproduction, (2) adaptation, (3) distribution, (4) performance, and (5) display.[17] The Copyright Act has been amended to include the DMCA.

The Digital Millennium Copyright Act (DMCA)

¶6 Congress enacted the DMCA on October 28, 1998 during the 105th Congress with the purpose of facilitating the "robust development and world-wide expression of electronic commerce, communications, research, development, and education."[18] Although the DMCA was meant to protect and foster electronic and digital developments, Congress realized that Internet intellectual property developments would be stifled if claims of copyright infringement fell upon the conduits of e-commerce, the ISPs.[19] For example, ISPs would be subject to claims of contributory and vicarious copyright infringement. In this sense, a chief purpose for enacting the DMCA was eliminating the possibility of bringing copyright infringement claims against ISPs for simply transmitting information over the Internet.

¶7 In order to prevail under contributory or vicarious infringement, a plaintiff must show "direct infringement by a third party."[20] A prima facie case of "direct infringement" can be shown by the plaintiff by establishing ownership of the infringed material and showing that the alleged infringers infringed on at least one of the exclusive rights stated in 17 U.S.C. § 106.[21] After the plaintiff establishes direct infringement and wishes to pursue a claim for contributory infringement, the plaintiff must show that the defendant knew or had reason to know of direct infringement, and induced, caused, or materially contributed to the infringement.[22] If the plaintiff wishes to pursue a claim of vicarious liability against the defendant, the plaintiff must show that the defendant had the right and ability to supervise the infringing activity and a direct financial interest in such activity.[23] The music industry successfully shut down Napster, a centralized server, by invoking the doctrines of vicarious and contributory liability.[24] Even though the music industry shut down Napster, illegal downloading of music continues to this day and in ever larger numbers since the development of P2P technology. P2P technology allows users to share files directly between individuals without the use of

---

[16] 17 U.S.C. §§ 101-122.
[17] § 106(1)-(5).
[18] Adams, *supra* note 13, at 213 (quoting S. Rep. No. 105-190, at 1, 105th Congress, 2d Session 1998).
[19] *Id.*
[20] A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 911 (N.D. Cal. 2000).
[21] Jennifer Norman, *Staying Alive: Can the Recording Industry Survive Peer-To-Peer?*, 26 Colum. J.L. & Arts 371, 372 (2003); *see* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001).
[22] Norman, *supra* note 21, at 372; *see Napster*, 239 F.3d at 1019; Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).
[23] *Id.*; *see Napster*, 114 F. Supp. 2d at 921.
[24] Norman, *supra* note 21, at 371.

a centralized server, thereby circumventing the possibility of secondary liability suits falling upon the P2P networks.[25] But ISPs, as conduits of both legal and illegal file-sharing, may face secondary liability suits.

¶8 Luckily for ISPs, the DMCA provides relief from the possibility of secondary liability suits. The DMCA amended Chapter 5 of the Copyright Act, creating § 512, "Limitations on Liability relating to material online." To combat the potentially damaging effect of direct, vicarious and contributory infringement that may fall upon ISPs and the Internet industry in general, Congress drafted the DMCA to limit the liability of ISPs for copyright infringement committed by their customers using the provider's systems or networks.[26] Under certain conditions, the DMCA affords copyright infringement immunity for ISPs by offering "monetary relief for direct, vicarious and contributory [copyright] infringement."[27] These "safe harbor" provisions will protect an ISP from claims of infringement if the ISP (1) does not have actual or constructive knowledge of the infringement, (2) does not benefit financially from the infringement, and (3) acts promptly upon notice of infringing material to remove, or prevent access to, the infringing material.[28] The "safe harbor" provisions do not necessarily require ISPs to seek copyright infringers, but do impose strong incentives upon ISPs to work with copyright owners.[29] Under § 512(i) of the DMCA, copyright holders can notify ISPs of infringing activities and ask courts to order the termination of infringing user's accounts.[30] In exchange for assisting copyright owners in identifying pirates who use the ISPs as avenues for infringement, ISPs are given protections against liability from copyright holders.[31] In order to receive protection from liability, ISPs must comply with a subpoena process which allows copyright holders to identify and pursue legal actions against pirates.[32] Specifically, § 512 allows copyright holders to issue subpoenas to ISPs demanding the name, address and telephone numbers of ISP subscribers suspected of illegally downloading copyrighted material.[33] The subpoenas can be filed prior to any claims of infringement, are not subject to judiciary review, nor require the alleged infringer to receive notice or opportunity to be heard. For these reasons, Verizon has challenged the subpoena powers of the DMCA.

THE VERIZON CASE

¶9 Until recently, the music industry avoided suing direct individual infringers for sharing copyrighted materials because of the tremendous cost and potentially disastrous publicity associated with filing lawsuits

---

[25] *Id.*
[26] *Verizon*, 240 F. Supp. 2d at 27.
[27] *Id.* (quoting S. Rep. No. 105-190, at 20).
[28] Adams, *supra* note 13, at 213; *see generally* 17 U.S.C. § 512.
[29] Adams, *supra* note 13, at 215; Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1176 (quoting H.R. Rep. 105-551(II), at 49; S. Rep. 105-190, at 20).
[30] 17 U.S.C. § 512(i).
[31] § 512(a)-(d).
[32] *See* § 512.
[33] *Id*.

against individual users.[34] However, the increase in illegal file sharing has forced copyright holders to sue individuals in order to protect copyright and the survival of the music industry. In order to bring a suit, a defendant must be identified.

¶10 On July 24, 2002, RIAA served a subpoena on Verizon Internet Services, Inc., seeking the identity of an anonymous copyright infringer allegedly using Verizon's network to impermissibly swap over 600 copyrighted files through P2P software provided by KaZaA.[35] The subpoena included a request for the user's specified Internet Protocol ("IP") address to enable Verizon to locate the computer where the infringements occurred. In addition to providing the time and date of the downloaded file, RIAA provided a declaration under penalty of perjury stating that the RIAA sought the identifying information in good faith and would use the information for the sole purpose of protecting the copyright of RIAA members.[36] Instead of providing the identifying information of the infringing user, Verizon refused compliance with RIAA's subpoena, stating that the subpoena powers of the DMCA did not apply to Verizon.[37] The issue surrounding the Verizon case, in essence, entailed "statutory interpretation relating to the scope of the subpoena authority under the DMCA."[38]

¶11 Under the DMCA safe harbor provisions, § 512(a)-(d), ISPs are given monetary, injunctive, and equitable relief from copyright infringement liablility. § 512(a), "Transitory digital network communications," provides ISPs with relief from liability "for infringement of copyright by reason of the provider's transmitting, routing or providing connections . . . or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections . . . ."[39] § 512(c), "Information Residing on systems or networks at direction of users," provides ISPs with relief from liability "for infringement of copyright by reason of the storage . . . of materials that resides on a system or network controlled or operated by or for the service provider . . . ."[40] In return for relief from liability, ISPs must abide by the DMCA subpoena power under § 512(h), which allows a copyright owner or person authorized to act on the owner's behalf to seek the identity of an alleged infringer by requesting the clerk of any United States district court to issue a subpoena to a service provider.[41] The proposed subpoena must contain, "a copy of a notification . . . ," and a sworn declaration stating that the subpoena will be used for the purpose of obtaining the identity of the alleged infringer and protecting the rights of the copyright holder.[42] Once issued, the

---

[34] Norman, *supra* note 21, at 392.
[35] *Verizon*, 240 F. Supp. 2d at 28.
[36] *Id*.
[37] *Id.* at 29.
[38] *Id.* at 26.
[39] § 512(a).
[40] § 512(c).
[41] § 512(h)(1).
[42] § 512(h)(2)(a)-(c).

subpoena authorizes and requires the ISP to "expeditiously disclose" information sufficient to identify the alleged infringer.[43]

¶12 Verizon's argument for not responding to the subpoena was based on the notion that it did not store any of the infringing user's files on its system; Verizon merely transmitted the allegedly infringing material.[44] Verizon argued that subsection (h) subpoena authority does not extend to subsection (a), dealing with transitory conduits, but is instead limited to subsection (c), providers that actively store allegedly infringing material.[45] Verizon viewed the DMCA's subpoena power as applying to Verizon only if the infringed material is stored or controlled by Verizon under subsection (c).[46] More specifically, Verizon stated that the infringed contents did not "reside on any system or network controlled or operated by or for [Verizon], but . . . are stored on the hardware of the Customer."[47] Verizon posited that since it only provided the alleged infringer with Internet connection and only transmitted the allegedly infringing material, Verizon's status fell under § 512(a) dealing with passive conduits, not under § 512(c) which deals with providers that store allegedly infringing material.[48] Therefore, Verizon contended, the subpoena power of subsection (h) did not apply because subsection (h) was limited to service providers storing material under subsection (c).[49]

¶13 RIAA simply argued that the DMCA subpoena power under § 512(h) applies to all service providers within the provisions of subsections (a) through (d), regardless of whether the infringing material is stored on or simply transmitted over the service provider's network.[50] Verizon's refusal to comply with the subpoena prompted RIAA to move the court pursuant to 17 U.S.C. § 512(h)(6) and Fed. R. Civ. P. 45(c)(2)(B) to enforce the subpoena.[51]

Court's Holding

¶14 In *Verizon*, the Court relied heavily on the legislative history of the DMCA, stating that Congress intended to create a tradeoff for ISPs through the DMCA in which the ISPs would receive "liability protections in exchange for assisting copyright owners in identifying and dealing with infringers . . . "[52] The Court then rejected Verizon's arguments and held that the subpoena power in 17 U.S.C. § 512(h) applied to "*all* Internet service providers within the scope of the DMCA, not just to those service providers storing

---

[43] *Verizon*, 240 F. Supp. 2d at 28; § 512(h)(3).
[44] Norman, *supra* note 21, at 393.
[45] *Id.; see* Opp'n of Verizon Internet Servs. to Mot. to Enforce ex Parte Subpoena at 3, Recording Indus. Ass'n of Am. (D.C. Cir. filed Aug. 30, 2002) (No. 1:02MS00323), *available at* http://www.eff.org/Cases/RIAA_v_Verizon.
[46] *Verizon*, 240 F. Supp. 2d at 29.
[47] *Id*.
[48] *Id*.
[49] *Id*.
[50] *Id.* at 29.
[51] *Id*.
[52] *Id.* at 37.

information on a system or network at the direction of a user.[53] The Court found Verizon's position to be lacking because it would "create a huge loophole in Congress' effort to prevent copyright infringement on the Internet."[54] The District Court granted RIAA's motion to enforce its subpoena and ordered Verizon to comply with the subpoena.[55]

John Doe Actions

¶15 The Court also rejected Verizon's call for John Doe actions in regards to claims against anonymous copyright infringers. Verizon suggested that as an alternative, RIAA should bring "John Doe" actions in federal court to obtain information identifying copyright infringers.[56] In "John Doe" actions, the copyright owner files a complaint against John Doe, the anonymous infringer. A third-party subpoena would then be issued and served upon the ISP pursuant to Federal Rule of Civil Procedure 45. The ISP would then notify their anonymous customer, John Doe, of the impending lawsuit.[57] Verizon argued that such procedures would offer both procedural and substantive protections in favor of the customer's rights, as well as providing the ISP the opportunity to quash the subpoena.[58] The Court rejected Verizon's procedural substitution and stated that John Doe actions would over burden the courts due to the vastness of copyright piracy on the Internet.[59] The Court added that John Doe actions would delay and undermine the copyright holder's ability to prevent and enforce their copyrights.[60]

CONSTITUTIONALITY OF THE DMCA SUBPOENA POWER

¶16 The Court noted that several *amici curiae* raised a number of possible issues involving the constitutionality of the DMCA subpoena powers. Ironically, Verizon never explicitly raised the constitutional issues. The Court stated that it was "wary of considering such issues"[61] but took it upon itself to address and settle the issue of the right to anonymous free speech within the Internet, stating that although there exists a constitutional right to remain anonymous in free speech, Verizon's customers who file-share copyrighted music are not using the Internet to express ideas.[62] The constitutional right to remain anonymous protects "those 'who support causes anonymously' and those who 'fear economic or official retaliation,' 'social ostracism,' or unwanted intrusion into 'privacy.'"[63]

---

[53] *Id.* at 26 (emphasis added).
[54] *Id.* at 35.
[55] *Id.* at 45.
[56] *Id.* at 39.
[57] *Id.*
[58] *Id.* at 40.
[59] *Id.*
[60] *Id.*
[61] *Id.* at 42.
[62] *Id.* at 43.
[63] *Id.* at 43 (quoting Watchtower Bible & Tract Soc'y of New York, Inc., v. Village of Stratton, 536 U.S. 150, 166 (2002)).

The DMCA and Anonymity

¶17 Although the District Court in Verizon touched upon the notion of "unwanted intrusion into privacy" in its opinion, the Court never addressed the privacy rights of the anonymous copyright infringers.[64] Since Verizon never raised these constitutional challenges in the case, RIAA did not brief the constitutional issues raised in the *amicus briefs*. However, proponents of privacy and anonymity on the Internet were unreceptive to the Court's rejection of John Doe actions. Proponents, such as Peter Swire who served in the Clinton Administration as Chief Counselor for Privacy and is currently a Professor of Law at the Moritz College of Law at Ohio State University, argue that the subpoena powers of the DMCA violate due process as well as privacy rights of individuals beyond the Internet because the identity of Internet users becomes available to almost anyone.[65] Swire predicts that the DMCA subpoena power will undermine and cause a chilling effect to First Amendment rights on the Internet because abusers of the DMCA subpoena powers can track identifying information back to anyone posting material on the Internet.[66] Furthermore, Swire predicts that putting the subpoena power in the hands of those without legitimate claims of copyright infringement will flood the federal courts with fraudulent requests, thereby making illegitimate claims indistinguishable from legitimate ones.[67] Chilling Effects Clearinghouse, a joint project by the Electronic Frontier Foundation and clinics of Harvard, Stanford, Berkeley, University of San Francisco, and University of Maine law schools, administered a searchable database for determining whether DMCA subpoenas and "Cease and Desist" letters were falsely or fraudulently issued to Internet users.[68] One example of an erroneous letter that Verizon heavily relies on involves an incident in which MediaForce, a security firm which searches for P2P nets for copyrighted works, acted on behalf of RIAA member Warner Brothers and sent a notice to an ISP, alleging copyright infringement of the film "Harry Potter and the Sorcerer's Stone."[69] The notice stated that MediaForce had a good faith belief that copyright infringement took place at a particular Internet Protocol address. The notice demanded that the service provider terminate the account of the person who had posted the alleged infringing material, which turned out to be a child's book report.[70] Other examples include claims made by the Church of Scientology aimed to remove links to websites written by individuals who publish

---

[64] *Id.*.
[65] Peter Swire, *Protecting Privacy from the "New Spam,"* THE BOSTON GLOBE, July 27, 2003, at E11.
[66] *Id.*
[67] *Id.*
[68] http://www.chillingeffects.org/.
[69] Br. for Appellant at 38-39, In re Verizon, 240 F. Supp. 2d 24 (D.D.C. 2003) (Nos. 03-7015, 03-7053 consolidated appeals).
[70] *Id.*

criticisms against the Church of Scientology and trademark claims made under the guise of copyright to take advantage of the DMCA (which applies solely to copyright).[71]

¶18 Proponents of Verizon's stance argue that the tremendous influx of "legally sanctioned harassment" will mirror that of "spam . . . limitless as the Internet itself."[72] For example, website operators would be able to identify their visitors for purposes such as marketing, stalking, and identity theft.[73] Verizon and its supporters also speculate that the DMCA subpoena power may extend to illegitimate claims of copyright, allowing "those who wish to silence their critics, retaliate against whistle-blowers, target purveyors of abortion literature, harass those who share politically damaging memos, stalk sexually-explicit photographers, remove personally embarrassing material, or accomplish other nefarious ends will use the DMCA subpoena process to un-mask their perceived foes."[74] In this sense, Verizon argues that the subpoena powers granted in § 512(h) are overly broad and will have chilling effect on the free speech of Internet users who wish to engage in legal activity but do not because they are scared that they will be subpoenaed.[75] More specifically, Verizon posited the possibility that copyright owners would wrongfully pursue and obtain the identity of non-infringing anonymous Internet users, thus discouraging Internet users from engaging in otherwise protected activity.[76]

¶19 The threat of superfluous suits and illegitimate claims of copyright infringement should not disturb the privacy rights of individuals because the DMCA contains provisions designed to prevent such illicit intrusions. In the *Verizon Second Subpoena Decision*, the District Court noted that DMCA § 512(h) provides protection for Internet users against "baseless or abusive subpoenas."[77] Not only is the subpoena applicant required to submit a notification similar to that of an actual copyright infringement complaint, but the subpoena applicant must also submit a sworn declaration stating that the subpoena and the identifying information obtained will "only be used for the purpose of protecting rights under [Title 17]."[78] These procedural safeguards aim to deter superfluous claims from reaching the courts. Furthermore, the anecdotal examples of fraudulent claims offered by Swire and Verizon do not require the invocation of the overbreadth doctrine. Verizon correctly pointed out the erroneous complaint in the "Harry Potter" incident; however,

---

[71] Br. of Amici Curiae in Supp. of Verizon's Opp'n to RIAA's Mot. to Enforce at 9, In re Verizon, 240 F. Supp. 2d 24 (D.D.C. 2003) (Civ. No. 1:02MS00323).
[72] Swire, *supra* note 65.
[73] *Id.*
[74] Br. of Amici Curiae in Supp. of Verizon's Opp'n to RIAA's Mot. to Enforce at 10, In re Verizon, 240 F. Supp. 2d 24 (D.D.C. 2003) (Civ. No. 1:02MS00323).
[75] Brief for Appellant at 39, In re Verizon, 240 F. Supp. 2d 24 (D.D.C. 2003) (Nos. 03-7015, 03-7053 consolidated appeals).
[76] *Id.*
[77] Br. of Amici Curiae Motion Picture Assoc. of Am., Inc. et al. at 14, In re Verizon., Nos. 03-7015, 03-7053 (consolidated appeals) (filed 2003) (quoting In re, Verizon Internet Services, Inc., 257 F. Supp. 2d 244, 263 (D.D.C. 2003)).
[78] 17 U.S.C. § 512(h)(2)(c).

Verizon incorrectly associated this error with the "notice-and-takedown" procedure of § 512(c)(3) instead of the subpoena section at issue, § 512(h).[79] The "Harry Potter" incident, as well as the other examples erroneous notices, involve notices that were served pursuant to § 512(c)(3) requesting ISPs to remove copyrighted material located on its servers.[80] Unlike § 512(h), a user's identity is not called for when a copyright owner invokes § 512(c)(3).[81]

¶20 Although the notions of fraudulent subpoenas and abuses of the DMCA are indeed worrisome, § 512(h) is not overly broad as Verizon and Swire predict because there is little proof of overbreadth and "the mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge."[82] In *Ashcroft v. American Civil Liberties Union (ACLU)*, the Supreme Court held that the overbreadth of a statute must be "real" and "substantial" in order to fail constitutional muster.[83] As the Supreme Court noted in *ACLU*, "anecdotes" of "questionable relevance to the matter at hand and certainly do not constitute a sufficient basis for invalidating a federal statute."[84] Indeed, the possibility of "legally sanctioned harassment"[85] should not constitute a prevalent part of daily internet use, but at this point, everyday illegal downloading and copyright infringement certainly overrides any prediction or anecdote offered by advocates of internet privacy. Furthermore, advocates of Internet privacy should not alarm themselves, or others, too much in regards to fraudulent issuances of subpoenas seeking identifying information from Internet users because courts will not tolerate false subpoenas.[86]

Privacy

¶21 Internet users should not be so alarmed by the fact that there is not 100% privacy on the Internet. Many Internet users find countless spam e-mails in their e-mail inbox everyday. Although senders of spam do not necessarily know the personal identity of those receiving such junk e-mail, ISPs certainly do. NetZero, an ISP, admits in their "Privacy Statement" that their customers are targets of customized advertisements.[87] Specifically, NetZero customers are given notice that NetZero will collect information about the users and

---

[79] Br. of Amici Curiae Motion Picture Ass'n of Am., Inc. et al. at 14-15, In re Verizon., Nos. 03-7015, 03-7053 (consolidated appeals) (filed 2003) (quoting *Verizon*, 257 F. Supp. 2d at 263).
[80] *Id*.
[81] *Id*.
[82] Members of the City Council of Los Angeles v. Taxpayers For Vincent, 466 U.S. 789, 800 (1984).
[83] Ashcroft v. American Civil Liberties Union (ACLU), 535 U.S. 564, 584 (2002) (quoting Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973) (The "overbreadth of a statute must not only be real, but substantial as well.")).
[84] *ACLU*, 535 U.S. at 585.
[85] Swire, *supra* note 69.
[86] *See* Bumper v. North Carolina, 391 U.S. 543, 549 (1968) ("A search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it turns out that the warrant was invalid."); Theofel v. Farey-Jones, 341 F.3d 978, 984 (9th Cir. 2003) (Subpoena may not have been coercive, but it was deceptive, and that is an independent ground for invalidating consent.).
[87] http://www.netzero.net/legal/privacy.html.

then disclose that information to advertisers.[88] Although this privacy matter involving NetZero differs from the present case involving Verizon, the common theme among all ISPs is that they all have access to the identifying information of their customers. Therefore, if an Internet user wishes to remain completely anonymous within the Internet, they must face the disappointing realization that their conduits into the Internet also act as the conduits into their personal information.

¶22 A District Court case, *McVeigh v. Cohen*,[89] demonstrated the notion that ISP customers will sometimes suffer the invasion of privacy by third parties and even by their ISPs. In *McVeigh*, plaintiff Senior Chief Timothy McVeigh sued America On-Line ("AOL") for the unauthorized disclosure of his personal information and sought to enjoin the United States Navy from discharging him based on his alleged homosexual conduct, a dischargeable offense.[90] After suspecting McVeigh of admitting homosexual conduct via the Internet, Lieutenant Karin S. Morean, a member of the Judge Advocate General's ("JAG") Corps, investigated the matter and requested a Navy paralegal to contact AOL and obtain the identification of an AOL subscriber who went under the screen name "boysrch."[91] The profile of "boysrch" included homosexual interests such as "collecting pics of other young studs" and "boy watching."[92] The profile did not contain any identifying information, such as the name, address, or phone number.[93] Before speaking to the plaintiff or requesting a warrant or court order, the Navy received affirmative indication from an AOL representative that the screen name "boysrch" belonged to the plaintiff.[94] Subsequently, the Navy sought to discharge McVeigh for violating the "Don't Ask, Don't Tell, Don't Pursue" policy.[95] In *McVeigh*, the Court evaluated the case under the Electronic Communications Privacy Act of 1986 ("ECPA"), which Congress enacted to address privacy concerns on the Internet and allow the government to obtain personal information about individuals from online service providers.[96] The Court in *McVeigh* held the Navy could have legally obtained the information of "boysrch" from AOL, but only if the Navy (a) obtained a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (b) gave prior notice to the online subscriber and then issued a subpoena or received a court order authorizing disclosure of the information in question.[97] Since the

---

[88] *Id.*
[89] 983 F. Supp. 215 (D.D.C. 1998).
[90] *Id*. at 218.
[91] *Id*. at 217.
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] The "Don't Ask, Don't Tell" policy allows gay service members to remain in the service despite being homosexual, allowing them to "serve their country honorably, so long as they are discrete in pursuing their personal lives." *McVeigh*, 983 F. Supp. at 220. However, if a service member conveys a propensity or intent to engage in homosexual conduct, then the service may discharge him or her. *Id.*
[96] *See* 18 U.S.C. § 2701 et seq.
[97] *McVeigh*, 983 F. Supp. at 219; *see* 18 U.S.C. § 2703(b)(1)(A)-(B), (c)(1)(B).

Navy did not perform either requirement prior to obtaining "boysrch's" identification, the Court granted McVeigh's Motion for a Preliminary Injunction and reinstated McVeigh into the Navy.[98]

¶23 Advocates of Internet privacy should not be shocked by the fact that third parties may obtain personal information from their ISPs. As *McVeigh* exemplifies, the subpoena power of the DMCA is not a novel instrument for obtaining the personal information of Internet users. Previous statutes enacted by Congress, such as the ECPA, illustrate the foresight of Congress to predict situations requiring the privacy rights of individuals to be encroached upon due to legal violations or infringements upon the rights of others. And given the noticeable lack of cases like *McVeigh*, the floodgates of false subpoenas seem to be fairly water tight.

VERIZON'S APPEAL SHOULD NOT SUCCEED

¶24 In April of 2003, the District Court of D.C. denied Verizon's request for a stay and ordered the company to comply with RIAA's subpoena.[99] Verizon then turned over the names of the copyright infringers but continues to appeal the matter.[100] Verizon is appealing the decision to the United States Court of Appeals for the D.C. Circuit, contending that the decision of the District Court would "open the floodgates of copyright holder,"[101] thereby undermining Internet user's confidence in the privacy of their Internet communications.[102] As a result, Verizon contends that consumer interest in broadband, an interest that the federal government has also pursued, would cease.[103] During the hearings on appeal, Verizon's counsel, Andrew McBride, argued that since the DMCA was written prior to Napster related copyright infringements in 1999, the DMCA was never intended to give copyright owners unrestrained access to the identities of Internet customers who use file-sharing services.[104] Don Verrilli, arguing on behalf of RIAA, countered Verizon's argument during the hearings and stated that Congress incorporated the subpoena power intentionally because Congress understood that copyright holders needed an effective tool to locate and identify the "digital thieves" stealing copyrighted material.[105]

¶25 The subpoena power should be upheld on appeal because the rampant piracy occurring over the Internet must cease. The music industry and the RIAA need the subpoena power to identify the numerous music pirates because the only ones who can pinpoint music pirates are the service providers. The RIAA

---

[98] *McVeigh*, 983 F. Supp. at 222.
[99] *Verizon*, 257 F. Supp. 2d at 275.
[100] David McGuire, *Verizon, Record Companies Duel Over 'Net Piracy*, WASH. POST, Sept. 16, 2003, *available at* http://www.washingtonpost.com/wp-dyn/articles/A20565-2003Sep16.html.
[101] Declan McCullagh, *RIAA Wins Battle to ID Kazaa User*, CNET NEWS.COM, *at* http://news.com.com/2100-1023-981449.html (last modified Jan. 21, 2003) (quoting Sarah Deutsch, Verizon's Vice President and Associate General Counsel).
[102] McGuire, *supra* note 116.
[103] *Id.*
[104] *Id.*
[105] *Id.*

admits that it does not want to resort to litigation, but in order to protect a product that is "regularly stolen,"[106] the copyright holder must take appropriate actions so as to prevent the downfall of their livelihoods. Even though the large record companies, whom much of the public disfavors, are experiencing the pains of piracy, smaller and independent parties and copyright holders, such as artists, songwriters, and everyone associated with the music industry, must also fight for their survival.[107] As the number of lawsuits and DMCA subpoena increase, Internet consumers must realize that the music industry is not attacking their privacy rights or attempting to gather personal information for the sake of mass marketing. Instead, Internet consumers must realize that the violations of copyright laws stemming from illegal downloading of copyrighted music have reached a critical stage. The large number of notices served and subpoenas issued does not indicate a problem with the subpoena powers of the DMCA. Rather, the large number of notices served and subpoenas issued reflects the immensity of the "piracy epidemic."[108] Unless stringent anti-piracy efforts, such as the identification of digital copyright pirates, continue on behalf of the artists that the Constitution specifically aims to protect, the sea of copyright will continue to be pillaged by those who seek to steal the fruits of creative and productive geniuses. If this wave of piracy does not cease or at least become deterred, the livelihoods of all those in the music industry will be washed away.

---

[106] http://www.riaa.com/news/newsletter/090803.asp
[107] *Id*.
[108] Br. of Amici Curiae Motion Picture Ass'n of Am., Inc. et al. at 15, In re Verizon, Nos. 03-7015, 03-7053 (consolidated appeals) (filed 2003).