IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., *Movant*, v. VERIZON INTERNET SERVICES, INC., *Respondent.*	Civ. No. 1:02MS00323

BRIEF OF AMICI IN SUPPORT OF VERIZON'S OPPOSITION TO RIAA'S MOTION TO ENFORCE

I. In This Case of First Impression, the Court Should Consider Anonymity Rights in Light of Peer-to-Peer Systems, Potential Abuse, and Amici Expertise.

This is a case of first impression. This Court is asked to enforce a pre-litigation subpoena seeking the identity of an Internet subscriber under a statutory provision, Section 512(h) of the Digital Millennium Copyright Act ("DMCA"), that was enacted in 1998 but which has never before been brought before a court. In addition to seeking the first-ever judicial enforcement of the statute, Movant Recording Industry Association of America ("RIAA") seeks to have this Court extend the reach of this never-before-enforced statute to a factual context that is far outside the landscape that confronted Congress when it passed the DMCA in 1998: an ISP who merely

serves as a conduit for a subscriber who offers allegedly infringing materials stored on his own computer via a peer-to-peer file sharing application ("P2P").[1]

Not only was the statute never intended to reach a situation in which the allegedly infringing material resides on the user's own computer rather than a computer owned or controlled by the ISP, but the application of the statute as RIAA urges highlights the constitutional infirmities of Section 512(h) itself.[2] The statute provides that, upon an unsupported allegation of copyright infringement by an Internet user on his own computer, a clerk of a court, without any substantive review by the court itself, must issue a subpoena to the user's ISP for the identity of the user.

Yet, under the Constitution, anonymous speech is protected. Thus, this case falls into the line of cases that have established safeguards for protecting the anonymity of Internet speakers who have not been shown to have engaged in any prohibited conduct. As the first case to consider such a request, this Court is faced with a simple, yet important, question: what is the constitutional protection for the anonymous speech of an Internet user when a copyright holder merely asserts, without evidentiary support, that he is offering to share infringing files on his own computer. Put another way, this Court is faced with the question of whether the DMCA standard should be different than the standard that has evolved in cases in which the identity of an anonymous Internet user is sought based upon claims of defamation, trademark infringement,

---

[1] Verizon addresses these statutory-construction issues. Amici focus on the constitutional free-speech and privacy issues of more direct concern to Internet users.

[2] In this brief, Amici argue only that Section 512(h) is unconstitutional in the context of Section 512(a), leaving to another day the broader question of whether Section 512(h) is unconstitutional under any component of the DMCA.

trade-secret violation, or violations of the securities laws. Amici urge this Court to reject RIAA's attempt to interpret Section 512(h) as an end-run around these constitutional protections.

In answering this question, it is significant to note that copyright owners like RIAA are not left without recourse. Without pre-litigation subpoena authority under the DMCA, RIAA can still obtain identifying information – common civil procedure rules have long provided routes for obtaining such information. Even if this Court adopts the interpretation of the DMCA advocated by RIAA, certain minimum due process protections (notice, opportunity to object, and judicial oversight) should be expressly adopted by this Court.

A. Amici Are a Broad Group of Consumer Rights Activists, Civil Liberty Protectors, and Technology Advocates.

Amici are a wide-ranging set of organizations concerned with the privacy of Internet users and the rights of consumers online. They file this brief in order to ensure that the Court carefully considers the rights not only of the individual whose identity is sought here, but of future individuals whose identity may be sought under Section 512(h).

Amici (in alphabetical order):

Alliance for Public Technology (APT) is a nonprofit organization of public interest groups and individuals. APT's members work together to foster broad access to affordable, usable information and communications services and technology for the purpose of bringing better and more affordable health care to all citizens, expanding educational opportunities for lifelong learning, enabling people with disabilities to function in ways they otherwise could not,

creating opportunities for jobs and economic advancement, making government more responsive to all citizens and simplifying access to communications technology.

For over 20 years, members of Computer Professionals for Social Responsibility (CPSR) have provided the public and policymakers with realistic assessments of the power, promise, and problems of information technology. CPSR members work to direct public attention to critical choices concerning the applications of information technology and how those choices affect society.

Consumer Alert, founded in 1977, is a non-profit, non-partisan consumer group. The organization takes a market-oriented view on public policy issues and provides consumer education materials.

Electronic Frontier Foundation (EFF) is a nonprofit public interest organization dedicated to protecting civil liberties and free expression in the digital world. With over 6,000 members, EFF represents the interests of Internet users in both court cases and the broader policy debates surrounding the application of law in the digital age. EFF opposes misguided legislation, initiates and defends court cases preserving individuals' rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to websites in the world, www.eff.org.

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has

participated as amicus curiae in numerous privacy cases, including most recently Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 122 S. Ct. 2080 (2002).

Media Access Project is a 30 year-old non-profit public interest law firm which represents the public's First Amendment rights to speak and to receive information through the electronic mass media. MAP has often depended on promises of anonymity to obtain information necessary to its representation.

The National Grange of the Order of Patrons of Husbandry (Grange) is the nation's oldest general farm and rural public interest organization. Originally founded in 1867, today the Grange represents nearly 300,000 individual members affiliated with 3000 local, county and state Grange chapters across the nation. The Grange has a strong interest in protecting the privacy rights of its members in rural areas who access the Internet through ISP services.

The National Consumers League is a private, nonprofit advocacy group representing consumers on marketplace and workplace issues. Our mission is to identify, protect, represent, and advance the economic and social interests of consumers and workers.

The Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy program, established in 1992, based in San Diego, Calif. It provides information and assistance to consumers on a variety of informational privacy issues including identity theft, telemarketing, Internet privacy, and financial privacy. It represents consumers' interests in public policy proceedings (legislative and regulatory agency) at the state and federal level.

Privacyactivsm is a non-profit organization dedicated to informing and empowering individuals about their privacy rights on the Internet. Through a mixture of education (using

graphics such as posters and video games), activism, and the law, the organization strives to make complex issues of privacy law, policy, and technology accessible to all. Privacyactivism can be found on the Internet at www.privacyactivism.org.

Public Knowledge is a Washington, D.C. based public-interest advocacy and research organization dedicated to fortifying and defending a vibrant "information commons" – the shared information resources and cultural assets that we own as a people. It works with diverse creators, consumers, civic groups and enlightened businesses to ensure that public access, creativity and competition are embodied in the digital age. One of its core goals is to ensure that intellectual property law and policy reflect the cultural bargain intended by the framers of the constitution: providing an incentive to creators and innovators while benefiting the public through the free flow of information and ideas.

The Utility Consumers' Action Network (UCAN) is a nonprofit membership organization based in San Diego, Calif. Established in 1983, it advocates for consumers' interests in the areas of energy, telecommunications, and the Internet.

B. This Controversy Should Be Decided in the Context of Peer-to-Peer Technology and Abuses of Internet Copyright Infringement Programs.

As noted above, P2P is a new phenomenon – it was not even a glimmer in anyone's eye when the DMCA was enacted. Equally important, P2P is the biggest revolution to happen on the Internet since the advent of email or the World Wide Web – millions of individuals use P2P now, and that number is growing exponentially. Incontestably, many P2P users swap infringing materials. But it is also beyond dispute that many P2P users do not swap infringing materials. P2P, like any basic computer functionality, is content-neutral. Like a Xerox machine or a VCR,

the software can be used for both infringing and noninfringing uses. KaZaA users have shared their own works, U.S. Government documents, including both the speech by President Bush after the September 11 attack, the speech by President Roosevelt after Pearl Harbor, authorized songs by artists, and the Prelinger Movie Archives.[3]

Although RIAA has moved to enforce a subpoena seeking only a single identity, its urged application of Section 512(h) should be considered in light of copyright owners' use of other DMCA provisions. Under the DMCA's provisions allowing copyright owners to require ISPs to take down allegedly infringing material [512(c)] and to terminate repeat infringers [512(i)], the RIAA, its sister organization for the motion picture studios, the Motion Picture Association of America (MPAA), and the corresponding organization for certain segments of the software industry, the Business Software Alliance (BSA), among others, have automated the processes outlined in the statute, flooding ISPs with demands. These massive copyright-enforcement programs have unleashed automated software ("bots") that speed across the information superhighway, reviewing all available filenames and related information. When these bots find a suspicious title or other information, they mark the location and automatically generate form notices to the ISPs under the DMCA.

Assessing a bot used by the MPAA, one report noted: the "Ranger [bot] is scouring the globe – Web sites, chatrooms, newsgroups and P2P –panning 60 countries, searching in English,

[3] These uses have been testified to in MGM et. al v. Grokster, et al., No. 01-08541 SVW (Central District of California) and are available at <http://www.eff.org/IP/P2P/MGM_v_Grokster/20020122_streamcast_memo_sum_judg.pdf> and <http://www.eff.org/IP/P2P/MGM_v_Grokster/20020122_prelinger_decl.html> (Prelinger Decl.).

Chinese, and Korean….Ranger is 24-7. Ranger is relentless. Ranger is a piece of software that acts like an Internet search engine… Ranger Online provides the data to the MPAA and prepares cease-and-desist letters….Last year, [MPAA] sent 54,000 letters; this year, it is on pace to send 80,000 to 100,000." *Ranger vs. the Movie Pirates, Software is Studios' Latest Weapon in a Growing Battle*, by Frank Ahrens, Washington Post, June 19, 2002, Page H01. And the MPAA only sends cease and desist letters for movies – this statistic increases many fold if one considers the bots used for music, software, and e-books. If the DMCA also permits P2P subpoenas, as RIAA argues here, the combined number of notices and subpoenas that ISPs will have to process could easily reach into the millions annually. The end result is that the Internet will change from a forum for the free exchange of ideas and information into a virtual surveillance state.

Significantly, neither the bots nor the copyright owners themselves download and review the suspicious file to determine if it satisfies the "substantial similarity" test under copyright-infringement law or if it carries any of the hallmarks of a fair use of the work, such as being a parody or a critical commentary about a work. Under the DMCA, the copyright owner need only have a "good-faith belief" of infringement; it is not expressly required to undertake any due diligence, such as actual review of the suspicious file, or consideration of potential fair use. An assertion of copyright infringement based solely on the title or other descriptive information about a file, rather than an individual review of the contents of the file itself, is problematic for obvious reasons – a "beetles" music file could be protected parody of The Beatles or a completely unrelated musical composition; a large file entitled "spiderman" could be an original multi-media work about a half-man-half-spider that poisons the world with tarantula-like venom,

or it could be a film-school documentary about an arachnologist, or it could be an infringing copy of the copyrighted movie.

Because the DMCA's low standard permits copyright owners to easily invoke its procedures, abuses and mistakes are legion.[4] This problem has been archived by the Chillingeffects.org project, administered by in part by EFF.[5] A few of the many examples follows:

- Notice ID No. 232 – Church of Scientology makes DMCA claims aimed at removing links to websites written by individuals who publish criticisms of the Church of Scientology.[6]
- Notice ID No. 310 – Individual asserts trademark claims as though they were copyright claims in order to take advantage of the DMCA, which applies only to copyright, not trademark, claims.
- Notice ID No. 312 - Individual uses DMCA in attempt to remove links to articles he wrote long ago and is now embarrassed about.
- Notice ID No. 94 – Copyright owner for the nationally syndicated cartoon character (annoyingly jolly purple dinosaur) threatens a DMCA notice to try to scare a criticism site

---

[4] These are just standard DMCA abuses under Sections 512(c) and 512 (i)– there will likely be many more if this Court opens the door to Section (h) subpoenas in the Section (a) context.

[5] Copies of the referenced notices are available at http://www.chillingeffects.org.

[6] See also *Google pulls anti-scientology links*, March 21, 2002, Matt Loney and Evan Hansen , News.com, Cnet, http://news.com.com/2100-1023-865936.html; *Google Yanks Anti-Church Site*, March 21, 2002, Declan McCullagh, Wired News, http://wired.com/news/politics/0,1283,51233,00.html; *Church v. Google How the Church of Scientology is forcing Google to censor its critics,* John Hiler, Microcontent News, March 21, 2002, http://www.microcontentnews.com/articles/googlechurch.htm.

into removing photo of Barney, saying that it "incorporates the use and threat of violence toward the children's character Barney without permission."[7]

- Notice ID No. 348 – DMCA claim made against individual who posted public court records that contained copyrighted images.

In short, if the history of the use of the Sections 512(c) and (i) provisions by copyright owners is any guide, and if the use of Section 512(h) is endorsed by this Court, the process for generating requests for pre-litigation subpoenas will be quickly automated. ISPs nationwide will receive hundreds, if not thousands of subpoenas, none of which are the result of an actual review of the content of an allegedly infringing file. Additionally, use of this identity-disclosure procedure will not be limited to legitimate claims of copyright infringement. Instead, 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. The DMCA subpoena process will often be employed without any genuine interest pursuing a legal remedy, i.e., often without any real intention to file a copyright-infringement action.

Because of these very-real dangers, and given the constitutional protections established for anonymous speech, the DMCA subpoena process as applied to Section (a) is unconstitutional. Purported copyright owners should not have the right to violate protected, anonymous speech with what amounts to a simple snap-of-the-fingers.

---

[7] *Lawyers Keep Barney Pure*, July 4, 2001, Declan McCullagh, Wired News, http://www.wired.com/news/digiwood/0,1412,44998,00.html.

II. The Constitutional Right to Anonymous Speech Is Grounded in Established Caselaw and Strong Underlying Rationale.

While RIAA's attempted expansion of the reach of Section 512(h) subpoenas to ISPs that only engage in "digital transmission" is troubling by itself, it is even more worrisome given the important constitutional rights of Internet users that are at stake and the failure of Congress to expressly provide any safeguards for those anonymous Internet users. Section 512(h) provides an extraordinary power to copyright holders: the power to require a court clerk to issue a subpoena, without any prior court review and before any litigation has commenced, in order to require a third party to provide the identifying information on an Internet speaker. No other federal statute of which Amici are aware grants such broad, unchecked pseudo-judicial power to private non-litigants.

Yet, while the pre-litigation nature of the subpoena is new under Section 512(h), courts have long considered situations where the identity of a potential litigant is unknown. Even in the relatively new context of the Internet, there is a growing body of law that balances the legitimate discovery needs of litigants with the right of anonymous speech and privacy rights of American Internet users. Section 512(h), regardless of any contrary statutory language, cannot be applied in a manner that outright disregards the constitutional rights of Internet users.

A. Wide-Ranging Caselaw Establishes Safeguards for Anonymous Speech.

Given our country's dedication to the unfettered exchange of ideas, the Supreme Court has held that the First Amendment requires protection for anonymous speakers. McIntyre v.

Ohio Elections Commission, 514 U.S. 334 (1995)(anonymous leafleting is protected speech); Talley v. California, 362 US. 60 (1960)(forced identification of handbill distributors violates right to anonymous speech); Buckley v. American Constitutional Law Foundation, Inc., 525 U.S. 182 (1999). The fundamental law protecting the right to speak anonymously was established during the dawn of this country's formation. Indeed, the anonymous pamphleteer is one of the enduring images of the American revolutionary heritage.[8] This country's protection for anonymous speech continues into the modern age. As recently as this year, the Supreme Court reaffirmed the constitutional right to anonymous speech. Watchtower Bible and Tract Society of New York Inc. v. Village of Stratton, 122 S. Ct 2080 (2002)(concluding that a city ordinance requiring pamphleteers to disclose their names to the city implicates "anonymity interests" that are rooted in the First Amendment).

The right to anonymity on the Internet has been given particular deference. The Supreme Court has looked on this aspect of the Internet with favor, recognizing that the Internet is "a democratic institution in the fullest sense; the World Wide Web constitutes a vast platform from which the public may address and hear from a worldwide audience of millions." Reno v. ACLU, 521 US 844, 853 (1997)("through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox.").

Online anonymity permits speakers to, for example, communicate unpopular or unconventional ideas without fear of retaliation, harassment, or discrimination, and to "disguise status indicators such as race, class, gender, ethnicity, and age which allow elite speakers to

[8] This historical scene is particularly apt here – Thomas Paine shared pamphlets, a P2P user shares files; both contain expressive content.

dominate real-world discourse." Lyrissa Barnett Lidsky, "Silencing John Doe: Defamation and Discourse in Cyberspace," 49 Duke L.J. 855, 896 (Feb. 2000). See also ACLU of Georgia v. Zell Miller, 977 F.Supp. 1228, 1230 (N.D. Ga. 1997)(recognizing constitutional right to communicate anonymously and pseudonymously on the Internet); ACLU v. Johnson, 4 F.Supp. 2d 1029, 1033 (D.N.M. 1998), aff'd 194 F. 3d 1149 (10th Cir. 1999))(upholding First Amendment right to communicate anonymously over the Internet); ApolloMedia Corp. v. Reno, 19 F. Supp. 2d 1081 (C.D. Cal. 1998), aff'd 526 US 1061 (1999); Anderson v. Hale, 2001 US.Dist. LEXIS 6127 (N.D. Ill. 2001.)(anonymous members of dissident group can claim privilege to quash subpoenas for their email addresses and online account information under the First Amendment).

Of course, this constitutional right to anonymous speech is not absolute. A person does not have the right to anonymously defame, infringe, extort, etc.[9] Nonetheless, as other courts have noted, "anonymity, once lost, cannot be regained" – it is necessary, therefore, to determine in advance if allegations of wrongdoing carry any weight before destroying the speaker's anonymity. Rancho Publications v. Superior Court, 68 Cal. App. 4th 1538, 1540-41 (1999)(court prevented discovery of identity of individuals who placed newspaper ad contained allegedly defamatory statements).

[9]RIAA should not be allowed to put the cart before the horse in arguing that a person has no right to anonymous speech for infringing use. This is precisely the point – no one has yet been shown to be an infringer. Given the First Amendment underpinnings of the right to anonymous speech, mere allegations cannot be sufficient to irreversibly extinguish a constitutional right.

For example, in a trademark-infringement case, Columbia Ins.Co. v. SeesCandy.com, 185 F.R.D. 573 (N.D.Cal. 1999), the court considered at length the necessary protections for an anonymous Internet speaker.[10] In the context of deciding whether a temporary restraining order should issue, the court faced the dilemma that the purported infringer was unidentified and un-served with the lawsuit. Given the anonymity of the defendant, the court took pause. "This need [to provide injured parties with a forum in which they may seek redress for grievances] must be balanced against the legitimate and valuable right to participate in online forums anonymously…This ability to speak one's mind without the burden of the other party knowing all the facts of one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit [or issue a subpoena] and thereby gain the power of the court's order to discovery their identity." Id. at 578.[11]

[10] A similar case also dealing with a plaintiff attempting to learn the identity of an anonymous Internet speaker that allegedly violated trade secrets is Prepaid Legal Services Inc., et al. v. Gregg Sturtz, et al., California Superior Court, CV 798295, heard July 13, 2001 (no published decision; Notice and Motion to Proceed under Pseudonym located at http://www.eff.org/Privacy/Anonymity/Discovery_abuse/PrePaid_Legal_v_Sturtz/20010712_motion_to_proceed.html).

[11] The Supreme Court has recognized the public interest in maintaining an appropriate balance in the copyright context as well, noting that "a successful defense of a copyright infringement action may further the policies of the Copyright Act every bit as much as a successful prosecution of an infringement claim by the holder of a copyright." Fogerty v. Fantasy, Inc., 510 US 517, 527 (1994)[not an anonymous speech case].

The SeesCandy court went on to explore the limiting principles that should apply when a party seeks to unmask an anonymous Internet speaker. These procedures were necessary to ensure that "the plaintiff has in good faith exhausted traditional avenues for identifying a civil defendant pre-service, and will prevent use of this method to harass or intimidate." Id. at 578. Specifically, the plaintiff should, first, identify the missing party with sufficient specificity such that the court can determine that the defendant is a real person or entity who could be sued in federal court and, second, identify all previous steps taken to locate the elusive defendant. Third, the plaintiff should establish to the court's satisfaction that the lawsuit could withstand a motion to dismiss. Notably in contrast to the DMCA, "a conclusory pleading will never be sufficient to satisfy this element…This is necessary …to prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant." Id. at 580-581. And, finally, the plaintiff should file a request for discovery with the court, along with a statement of reasons justifying the specific discovery sought.

Section 512(h) does not even begin to satisfy these requirements. Indeed, the DMCA subpoena provision only requires simple paperwork to be filed, and for the copyright owner to make a self-serving, utterly conclusory statement about his good-faith belief that the material is infringing. This is particularly true here, when the copyright owner has not even asserted that the supposedly infringing files meet the "substantially similar" test of copyright infringement (which cannot be done without reviewing the files first), or asserted that such file-sharing was done for a

commercial purpose.[12] It is inappropriate to breach constitutional rights based on mere allegations of wrongdoing. Otherwise, rights will be too easily shattered based on spurious claims.[13] And once anonymity has been violated, effective remedies are difficult to devise (the "cat out of the bag" syndrome). Genuine copyright owners pursuing legitimate instances of infringing P2P activity will be able to easily meet these SeesCandy requirements. And, in doing so, the constitutional rights of anonymous Internet speakers will be sufficiently protected.

Similarly, the New Jersey appellate court recently issued an extensive opinion regarding the rights of anonymous Internet speakers in the defamation context. In Dendrite International v. Does, 342 N.J. Super 134, 141-142 (N.J. Super AD. 2001), the appellate court adopted a four-part test to ensure that the right to speak anonymously can be lost only if the plaintiff can show that it has a valid case against a speaker that could not be pursued without identifying the speaker. Under this Dendrite test, the plaintiff is first required to notify the anonymous speaker that his identity is being sought and give him an opportunity to oppose the request. Next, the plaintiff must identify the exact statements alleged to be unlawful. The court must then decide both whether the complaint states a valid claim for relief and whether the plaintiff has enough evidence to support its claim. Finally, if these first three criteria are met, the court must balance the individual's First Amendment right of anonymous speech against the strength of the case and the necessity of identifying the speaker.

---

[12] RIAA's likely argument that "if it quacks like a duck and walks like a duck, it is a duck" should not be sufficient to override constitutional speech rights, especially when RIAA is perfecting capable of examining the creature.

[13] As noted earlier, P2P users number in the millions, so any such framework could have a devastating chilling effect on Internet speech.

Here, it is plain that the Section 512(h) subpoena process also does not meet the requirements of Dendrite. The statute does not require that any notification be given to the speaker, either by the copyrightholder or the ISP. The purpose of this notice requirement is to give the speaker the chance to clear up any mistakes of fact or law underlying the claim before his identity is revealed. These could include an error in the IP address, a fair-use claim, or a jurisdictional defense. Next, Section 512(h) fails to provide for any judicial review of the allegations of the copyright owner, and instead requires the subpoena to be issued as a mere ministerial matter by the court clerk. Finally, and most importantly, the statute fails to provide for any "balancing" of the individual's First Amendment rights against the strength of the case and the necessity of identifying the speaker. Indeed, the copyright holder need not even assert that it intends to sue the user, something required by FRCP 27(1) for pre-litigation discovery. Petition of Ingersoll-Rand Co., 35 F.R.D. 122 (1964).

Similarly, In re Subpoena Duces Tecum to America Online, Inc., 52 Va Cir. 26, WL 1210372, (Va. Cir. Ct. 2000), also recognized the constitutional dimension inherent in anonymous Internet speech. "To fail to recognize that the First Amendment right to speak anonymously should be extended to communications on the Internet would require this Court to ignore either United States Supreme Court precedent or the realities of speech in the twenty-first century." Id. The court reviewed a subpoena seeking the identity of certain Doe defendants who had allegedly made defamatory statements online. The Virginia court applied a two-part test to determine whether the subpoena would be enforced. According to its formulation, the court

must first be convinced by the pleadings and the evidence submitted that the party requesting the subpoena has a legitimate, good-faith basis for doing so. Importantly, it was the court itself, not a self-interested party or an untrained court clerk, that made this determination. Second, the court required that the subpoenaed identity information be central to the dispute.

And again, in Doe v. 2TheMart Inc., 140 F.Supp. 2d 1088 (W.D. Wash. 2001), the court imposed a strict burden on a party seeking identifying information about an Internet speaker who allegedly violated securities laws. The court held that, where a party seeks information about a non-party anonymous Internet user, the party seeking the identifying information must establish to the court that (1) the subpoena was issued in good faith and not for any improper purpose; (2) information sought relates to a core claim or defense; (3) the information sought is directly and materially relevant to the claim or defense; and (4) the information sufficient to establish or to disprove the claim or defense is unavailable from any other source. This court noted that the standard for disclosing the identity of a person that is not a party to a lawsuit is particularly high. "Non-party disclosure is only appropriate in the exceptional case…This Court is mindful that it is imposing a high burden 'but the First Amendment requires us to be vigilant in making [these] judgments, to guard against undue hindrances to…the exchange of ideas.'" Id. at 1095.

Although the tests vary somewhat, all of them share a key critical characteristic that is absent from Section 512(h): the requirement that a court of law review the evidence and allegations and balance them with the constitutional right of anonymous speech before the anonymity of an Internet user is breached. It is for this fundamental reason that Section 512(h) cannot be constitutionally expanded to reach Section 512(a).

B. The Rationale for Protecting Anonymous Speech Resounds in Free Speech and Privacy Concepts.

The rationale underlying the right to anonymous speech comes from two important wellsprings of constitutional law: free-speech and privacy interests.

For free-speech, it is self-evident that some individuals will not participate in socially beneficial discourses if they must identify themselves or think that their identity will be easily learned. This intimidation effect is not a casual matter – the Supreme Court itself has recently reiterated the crucial role that the unfettered exchange of ideas plays in our society, stating, "The citizen is entitled to seek out or reject certain ideas or influences without [undue] government interference or control." United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 817 (2000). See also Winters v. New York, 333 US 507, 510 (1948)("What is one man's amusement, teaches another's doctrine…"); Griswold v. Connecticut, 381 US 479, 482 (1965)("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read…and freedom of inquiry…").

As another jurist noted, "…the spectre that a government agent will look over the shoulder of everyone who reads…Fear of criticism goes with every person into the bookstall. The subtle, imponderable pressures of the orthodox lay hold. Some will fear to read what is unpopular, what the powers-that-be dislike…[F]ear will take the place of freedom in the libraries, bookstores, and homes of the land. Through the harassment of hearings, investigations, reports, *and subpoenas*, government will hold a club over speech…" United States v. Rumely, 345 US 41, 57-58 (1953)(Douglas, J., concurring)(emphasis added). See Julie Cohen, A Right to

Read Anonymously: A Closer Look at Copyright Management in Cyberspace, 28 Conn. L. Rev. 981, 1007-1008 (1996).

An individual's right to privacy is also implicated when his anonymity is stripped without due justification. An individual's privacy interest is shaped by his reasonable expectations. Courts have held that a person has a "reasonable expectation" of privacy where first, he has exhibited an actual (subjective) expectation of privacy and, second, society is prepared to recognize that expectation as "reasonable." Katz v. U.S., 88 S. Ct 507, 361 (1967)(Justice Harlan, concurring with Majority; use of electronic listening device violated reasonable expectation of privacy in telephone-booth conversation); California v. Ciraolo, 476 US 207, 211 (1986), People v. Ayala, 96 Cal. Rptr. 2d 682 (Cal. 2000).

P2P files can be revealing, or misleading. For example, if an individual has a bunch of gangsta rap files available through P2P on his computer, one might form a misleading opinion of him, if it was not also known that he had those files in order to teach his seminar class on the perceptions of African-American culture in modern society. One author has described this problem well: "Even if the books we [own] aren't in any way embarrassing – *Memoirs of a Geisha* [for example] is a well-regarded novel – we run the risk of being stereotyped as the *kind* of person who would [own] a particular book or listen to a particular song. In a world in which citizens are bombarded with information, people form impressions quickly, based on sound bites, and these impressions are likely to oversimplify and misrepresent our complicated and often contradictory characters. Jeffrey Rosen, The Unwanted Gaze, p. 9 (Random House, pub. 2000).

The average individual does not expect that his identity will be disclosed by his ISP when he shares files in a P2P system. After all, his ISP in this transaction is nothing more than a wire

that gives him a connection to the Internet, and that has no knowledge of, storage of, or content-association with his P2P transaction. To the average individual, the technical framework and role of an ISP in this context is similar to the telephone company, providing little more than a dial tone -- an individual does not reasonably expect AT&T to disclose that he called a woman not his wife at midnight on April 3, 2001 and spoke for 20 minutes about a trip to Hawaii.

Protecting the individual's realm of privacy is especially important in the digital age. "Our secrets, great or small, can now without our knowledge hurtle around the globe at the speed of light, preserved indefinitely for future recall in the electronic limbo of computer memories. These technological and economic changes in turn have made legal barriers more essential to the preservation of our privacy." Shulman v. Group W Productions, Inc., 18 Cal. 4th 200, 243-244(1998)(J. Kennard, concurring).

In light of the rationale for privacy, free speech, and ultimately, anonymous speech, the DMCA subpoena provision in the context of Section (a) should be deemed unconstitutional.

C. Because the DMCA Subpoena Provision Is Saturated with Constitutional Problems, Legal Doctrines of Statutory Interpretation Require a Narrow Construction of the DMCA Statute.

For the reasons outlined above, the DMCA subpoena power violates individual's constitutional anonymous speech rights. In order to avoid such fundamental violation, this Court should adopt the narrow construction advocated by Verizon.

In Schneider v. Smith, 390 US 17 (1968), the Supreme Court narrowly construed a statute granting investigatory authority (the equivalent of judicial discovery) into 'subversive' activities, to preclude a broad authorization to 'probe the reading habits' of individuals. As the

Court noted, "It is part of the stream of authority which admonishes courts to construe statutes narrowly so as to avoid constitutional questions." Id. at 26. When a court faces a choice between two conflicting statutory interpretations, it should favor the interpretation that avoids or reduces constitutional concerns, if possible. INS v. St. Cyr, 733 US 289 (2001); New York v. Ferber, 458 US 747, 769 n.24 (1982)(when interpreting federal statutes that implicate First Amendment interests, courts should "construe the statute to avoid constitutional problems, if the statute is subject to such a limiting construction").

Moreover, the Supreme Court has held that a court order compelling production of information under circumstances that would threaten the exercise of a fundamental right is "subject to the closest scrutiny." NAACP v. Alabama, 357 US 449 (1957)(forced identification of NAACP members violates freedom of assembly). In other words, when fundamental expressive rights are implicated, courts require that government action be no broader than necessary. See Shelton v. Tucker, 364 US 479, 488 (1960), Buckley v. Valeo, 424 US 1 (1976)(least restrictive means test).

Furthermore, it is highly questionable whether the DMCA subpoena provision is constitutionally permissible as to any part of the DMCA, not just as applied to Section (a).[14] For example, it is unknown if an Internet user is subject to this Court's, or any court's, jurisdiction, and the subpoena power of a court cannot be more extensive than its jurisdiction. United States Catholic Conference v. Abortion Rights Mobilization, Inc., 487 US 72, 76-77 (1988). Certainly

[14] As noted earlier, Amici are not here challenging the constitutionality of Section (h) in its entirely; Amici's constitutionality challenge is only as to the application of Section (h) to Section (a). Nonetheless, questions about Section (h)'s overall validity counsel in favor of a narrow construction.

a freestanding subpoena provision, separate and apart from any on-going or contemplated litigation, raises grave concerns. Houston Business Journal, Inc. v. OCC, 86 F.3d 1208, 1212-13 (D.C. Cir. 1996)("[t]he federal courts are not free-standing investigative bodies whose coercive power may be brought to bear at will in demanding documents from others."). See also United States v. Morton Salt Co., 338 U.S. 632, 641-43 (1950)(because "[t]he judicial subpoena power…is subject to those limitations inherent in the body that issues them because of the provisions of the Judiciary Article of the Constitution," federal courts are "reluctant if not unable to summon evidence until it is shown to be relevant to issues in litigation").

In sum, Section 512(h) is constitutionally infirm, at least as applicable to Section (a). It compels revelation of a person's identity based on that person's speech activity without due regard for that individual's constitutional rights to anonymity. Thus, this Court should ensure that the DMCA subpoena provision is construed in the narrowest possible manner. Verizon's interpretation of the statute – that identity disclosure may be invoked pursuant to Section (h) only when the infringing materials actual reside on the ISP's network and therefore Verizon can independently corroborate that an infringement occurred – limits the problems of unsupervised use of judicial power to violate the constitutional right to anonymous speech.

III. Copyright Owners Are Not Precluded from Identifying Anonymous Internet Infringers Simply Because the DMCA Subpoena Power Does Not Apply to P2P.

Although statutory interpretation and constitutional rights to anonymous speech prohibit RIAA from expanding the DMCA subpoena provision to P2P users, RIAA is not foreclosed from pursuing alleged infringers or learning their identities. All RIAA needs to do is file a simple lawsuit or seek pre-litigation discovery under the Federal Rules of Civil Procedure.

Lawsuits with fictitiously named defendants are permitted when the plaintiff is unable to otherwise identify the defendant. See Rosenberg v. Crandell, 56 F.3d 35, 37 (8th Cir. 1995)(permitting a suit naming fictitious parties as defendants to go forward because the allegations in the complaint were "specific enough to permit the identity of the party to be ascertained after reasonable discovery"). In fact, such suits are so common, they are routinely called John Doe cases. With the advent of the Internet, such cases have become practically routine.

RIAA cannot be heard to complain that filing a lawsuit puts it in a catch-22 situation because discovery is stayed until the Summons and Complaint are served on the defendant and a short period thereafter.[15] This stay is not determinative in a John Doe case because all court rules of which Amici are aware allow a plaintiff to go into court, on an ex parte basis, to seek leave to issue a regular subpoena in order to identify a Doe defendant. "As a general rule, discovery proceedings take place only after the defendant has been served; [but] courts have

[15] In this Court, discovery would be stayed until the defendant is served with the lawsuit and the parties have conducted the Initial Conference. See, e.g., Fed.R.Civ.Proc. 33(a)("Without leave of court or written stipulation, interrogatories may not be served before the time specified in Rule 26(d).").

made exceptions, permitting limited discovery to ensure after filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant. Columbia Insurance v. SeesCandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999).

Alternatively, RIAA could seek discovery under Rule 27 of the Federal Rules of Civil Procedure. This Rule allows discovery prior to the filing of a lawsuit, contingent on certain protections for the unknown parties. Rule 27 requires that the petitioner have a sufficiently serious claim that he expects to file a lawsuit but is presently unable to file, a description of the contemplated lawsuit, and a description of the sought-for discovery. Significantly, the dangers of unilateral, unsupervised discovery are such that the Rule requires that notice be provided to the extent possible, and provides for appointed counsel to represent the unserved parties.

These standard court procedures to obtain identity information are better suited to guard against unjustified constitutional intrusions. In light of the constitutional rights implicated by anonymous speech, judicial oversight lends an important step in this system of checks and balances, even if, as a practical matter, the judicial approval of such subpoenas becomes routine. California Shellfish, Inc. v. United Shellfish Co., 56 Cal. App. 4th 16 (1997), explains the rationale well: "Allowing a plaintiff to initiate discovery by deposition subpoena…before serving any defendant with the summons and complaint, and without notice of the deposition to any defendant, or any other party in the action, is fraught with the danger for abuse recognized by our Supreme Court years ago. `If a party were allowed to compel an independent witness to give his deposition, all without notice to the opposing party, a situation not contemplated by the

discovery statues would result. For then a party might resort to all manner of discovery without adequate protection to his opponent, so long as he intended to forego any formal introduction of the material at time of trial. This would present an intolerable situation.' A calculating litigant might conclude that it could benefit from the opportunity to access information it might not otherwise have if an adversary were on notice of the litigation and able to raise valid objections." Id. at 24.

It is only when a court is presented with an ex parte request to issue a subpoena prior to service of a lawsuit (or prior to the filing of a lawsuit) that a neutral and learned arbiter can evaluate the matter. Certainly neither RIAA nor Verizon can adequately replace the objectivity or constitutional sensitivity of an Article III court. Moreover, neither have any incentive to do so. RIAA obviously cannot maintain a fully neutral perspective in claiming that its copyrights have been infringed. Verizon is unlikely to expend its own resources to scrutinize the legitimacy of the thousands, if not hundreds of thousands, of subpoenas that it receives.

Only a judge, and not a court clerk, can bring the necessary knowledge of the legal system to bear. A court can assess the strength of the case presented, the interest of the user in anonymous speech, and the issues of protected criticism, parody, or other instances of "fair use." The judge is also well-situated to consider jurisdiction, verify that a movant is not masquerading as a copyright owner, and catch typographical or other errors.[16]

[16] Typographical errors are frequent in Internet cases because tracking an anonymous user often means relying on long strings of numbers, namely the Internet Protocol (IP) address, time, and date. For instance, in this case, RIAA requested that Verizon identify the user "at IP address: 141.158.104.94 on 7/15/02 at 5:26 p.m. (EDT)." See RIAA's Attachment B.

In addition, by requiring that the matter come before a judge, and be filed as a true pleading, copyright holders – or, at least, their attorneys - are less likely to intentionally or negligently pursue P2P users engaging in protected activity. Knowing that a judge acts as a gatekeeper, and that they face malicious-prosecution claims, evidentiary exclusions, ethics complaints, and Rule 11 sanctions, the number of requested subpoenas will likely be greatly reduced – and the underlying copyright violations will be more certain.[17]

IV. If This Court Determines that the DMCA Subpoena Provision Does Apply to "Transitory Digital Network Communications," the Court Should Still Require Compliance with Procedural Due Process.

If this Court concludes that the DMCA subpoena provision is properly interpreted to cover Section (a), and if this Court concludes that individual anonymous-speech rights do not make the subpoena provision unconstitutional (at least as applied to P2P), then this Court should nonetheless enforce the subpoena subject to mandates of procedural due process.

Under procedural due process, a person who has been deprived of "liberty or property" is entitled to certain due process. The type of process required depends on the circumstances. To identify the specific procedural protections due, courts consider (a) the private interest that will be affected by official action; (b) the risk of erroneous deprivation of such interest through the

[17] The DMCA's "good faith" requirement may not require "due diligence" or affirmative considerations of whether the activity is protected under the fair-use doctrine. In contrast, FRCP 11 requires "best of the signer's knowledge, information and belief formed *after reasonable inquiry*, it is well grounded *in fact* and *is warranted by existing law*…" (emphasis added). In addition, under the DMCA, penalties attach only if the copyright owner "knowingly, materially" misrepresents an infringement, so the copyright owner is motivated to not carefully investigate a claim before seeking to enforce a DMCA right. See Section 512(f).

procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and (c) the government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements would entail Matthews v. Eldridge, 424 U.S. 319, 335 (1976) citing Goldberg v. Kelly, 397 U.S. 254 (1970).

As a result of the DMCA subpoena provision, an individual is at risk of losing a constitutional right, his right to anonymous speech. The risk of erroneous violation of this right is high, given the fact that it is sought by a self-interested party and issued by a court clerk without scrutiny. This risk can certainly be greatly reduced if the procedures outlined by the SeesCandy, Dendrite, 2theMart, and America Online, Inc. courts are adopted. In particular, the government has a strong interest in seeing that the judicially empowered discovery processes are properly used. Indeed, in discovery, "[t]here is an opportunity for litigants to obtain…information that…could be damaging to reputation and privacy. The government clearly has a substantial interest in preventing this sort of abuse of its processes." Seattle Times Co. v. Rhinehart, 467 US 20, 35 (1984). Finally, the burden on the judicial branch in adopting these protections is minimal in so far as it entails adoption of three requirements: judicial oversight, notice to the user, and a right to object.

The essence of due process is the requirement that a person at risk of deprivation be given notice of the deprivation against him and a meaningful opportunity to contest it. Joint-Anti Fascist Comm. V. McGrath, 341 U.S. at 171-172; Mullane v. Central Hanover Bank & Trust Co., 339 US 306 (1950). The more serious the interest involved, the more procedural protections will apply. Irwin v. City of New York, 902 F.Supp. 442 (S.D.N.Y. 1995). In addition, depending on the seriousness of the interest involved and the costs involved, due process may require a pre-

deprivation hearing. The timing and content of the notice and the nature of the hearing depend on a balancing of the interest or liberty involved and the costs involved. Goss v. Lopez, 419 U.S. 565 (1975). For instance, a full evidentiary hearing has been required before termination of a welfare recipient's benefits. Goldberg v. Kelly, 397 U.S. 254 (1970). Pre-deprivation hearings have been required before employment termination. Perry v. Sindermann, 408 U.S. 593 (1972).

For DMCA subpoenas, procedural due process requires, at a minimum, the following: (1) ISP or copyright owner must give notice of the clerk-stamped subpoena to the subscriber (notice to be provided by mail and confirmed-receipt email to the extent possible); (2) the subscriber must have a reasonable opportunity (e.g., 15 days) to object to the clerk-stamped subpoena. It is particularly crucial that an anonymous speaker be provided with these basic safeguards, because, otherwise, the anonymous person who is illegitimately identified *never* has a chance to protect his constitutional right. Unlike the situation in Perry, which requires a pre-deprivation hearing before job termination, the anonymous person cannot re-gain what he has lost. Finally, procedural due process requires (3) if ISP or subscriber objects to the clerk-stamped subpoena, issuing party must file a motion to enforce it with the court, in order that the court may weigh the competing constitutional claims. Because such a motion will be the first time that a court will have evaluated the competing claims and presented with an opportunity to issue an order, neither the subpoena recipient nor the subpoena target should face any danger of being held in contempt of court for challenging the initial clerk-stamped subpoena.

Undoubtedly, RIAA will object to even these minimal due process protections. RIAA is sure to note that the DMCA statute states that the court clerk should issue and the ISP should

respond to the subpoena "expeditiously." Nonetheless, the DMCA is not exempt from procedural due process requirements. "Expedite" cannot mean "railroad."

V. Conclusion.[18]

In this case of first impression, RIAA seeks to expand a DMCA subpoena provision of dubious legal validity to potentially millions of anonymous P2P users in which an ISP has only a passing connection. Because of the constitutional right to anonymous speech, RIAA's subpoena expansion should not be permitted.

As set forth in the multi-factor tests in SeesCandy, Dendrite, and other cases, before the cloak of anonymity can be tossed aside, the facts and law must first be marshaled and scrutinized by a court, ultimately balancing First Amendment rights against competing concerns. Given Section 512(h)'s failure to incorporate any of these safeguards, the statute, at least as applied to Section (a), is unconstitutional. This determination causes no legally cognizable injury to copyright owners, because they may pursue redress and discovery procedures through the same court system that every other injured party uses. It is only a court, with its impartiality and reasoned consideration, that is the appropriate forum to determine the competing claims of adversarial parties.

In the alternative, if this Court rules otherwise, it should nonetheless ensure that procedural due process is expressly grafted into the DMCA subpoena provision. At a minimum,

[18] Amici note that the Court granted RIAA's motion for expedited briefing, giving Amici only a few days to prepare this brief. Should the Court find it useful, Amici are willing to provide supplemental briefing. Amici are also aware of other third parties that are interested in joining this brief, but were unable to do so at this time because of time constraints.

procedural due process in this situation requires notice, an opportunity to object, and judicial review of any ensuing dispute.

Without these minimum protections, a surveillance society is the almost-certain consequence of permitting any purported copyright owner the right to subpoena a P2P user's identity information.

Pursuant to Local Rule 7.1, Amici request oral argument on this matter.

By _____
Joe Robert Caldwell, Jr.

Joe Robert Caldwell, Jr.
LOCAL COUNSEL
(DC Bar No. 965137)
Baker Botts LLP
The Warner
1299 Pennsylvania Ave., NW
Washington, DC 20004
(202) 639-7700

Megan E. Gray
HAC VICE COUNSEL
(DC Bar No. 478479)
GRAY MATTERS
1928 Calvert St. NW, Suite 6
Washington, DC 20009
(202) 265-2738
Fax (202) 265-0954

Attorneys for Amici Parties
Alliance for Public Technology (APT), Computer Professionals for Social Responsibility (CPSR), Consumer Alert, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Media Access Project, National Grange of the Order of Patrons of Husbandry, National Consumers League, Privacy Rights Clearinghouse, Privacyactivism, Public Knowledge, and Utility Consumers' Action Network (UCAN)

CERTIFICATE OF SERVICE

I certify that copies of the foregoing BRIEF OF AMICI PARTIES IN SUPPORT OF VERIZON'S OPPOSITION TO MOTION TO ENFORCE SUPBOENA were sent via facsimile (or email, per counsel's request) and first-class mail on August ____, 2002, to:

Donald B. Verrilli, Jr.
Thomas J. Perrelli
Cynthia J. Robertson
JENNER & BLOCK
601 Thirteenth Street NW
Suite 1200
Washington, DC 20005

Counsel of Record for Movant
Recording Industry Association
of America (RIAA)

William D. Iverson
Timothy C. Hester
Donald J. Ridings, Jr.
COVINGTON & BURLING
1201 Pennsylvania Avenue NW
Washington, DC 20004-2401

Counsel of Record for
Respondent Verizon Internet Services, Inc.

_____
Megan E. Gray

DC01:335561.1