LIBERTY UNIVERSITY

Liberty University Law Review

Volume 5 | Issue 3 Article 7

July 2010

Let the Pirates Fend for Themselves: Arista Records v. Does 1-16 and Dispelling the Internet's Ring of Gyges Myth

Daniel J. Yamauchi

COMMENT

LET THE PIRATES FEND FOR THEMSELVES: *ARISTA RECORDS V. DOES 1-16* AND DISPELLING THE INTERNET'S RING OF GYGES MYTH

Daniel J. Yamauchi[†]

I. INTRODUCTION

The lure of invisibility, or its more realistic cousin *anonymity*, is no new temptation; individuals have desired and pursued various levels of privacy throughout history for a myriad of reasons. While many motives are perfectly acceptable and uncontested, the coveted veil of anonymity provides a tempting advantage: the unknown man is unaccountable.[1] In the *Republic*, Plato references the mythological "Ring of Gyges"[2] to explore the nefarious effect of this unusual power and its ethical implications.

> Suppose now that there were two such magic rings [granting invisibility], and the just put on one of them and the unjust the other; no man can be imagined to be of such an iron nature that he would stand fast in justice. No man would keep his hands off what was not his own when he could safely take what he liked out of the market, or go into houses and lie with anyone at his pleasure, or kill or release from prison whom he would, and in all respects be like a god among men. Then the actions of the just would be as the actions of the unjust; they would both come to last at the same point. And this we may truly affirm to be a great proof that a man is just, not willingly or because he thinks that

---

† Editor-in-Chief, LIBERTY UNIVERSITY LAW REVIEW, Volume 5. J.D. (2011); Liberty University School of Law; B.A., University of Arizona. I dedicate this Comment to my parents for their unwavering love, support, and encouragment, and to the Warrens for providing me a home away from home. Thank you to Andrew Connors, Matthew Hegarty, and Ben Walton for your editorial guidance, mentoring, and friendship. *Psalm* 115:1.

1. To be more precise, this statement should be qualified to reflect that one remains unaccountable *only to other men*. For Christians, the Bible explicitly acknowledges that God is omnipresent, and nothing can be hidden from his view: "Woe to those who deeply hide their plans from the LORD, And whose deeds are done in a dark place, and they say, 'Who sees us?' or 'Who knows us?'" *Isaiah* 29:15 (NASB).

2. The accepted title for this legend derives from chapter ten in a dialogue discussing how Gyge's ring empowered Hades when he placed it on his helmet, thus rendering him invisible. PLATO, *Republic: Book II*, *in* FIVE GREAT DIALOGUES 253, 484 (Louise Ropes Loomis ed., B. Jowett trans., 1942).

> justice is any good to him individually, *but of necessity, for wherever anyone thinks that he can safely be unjust, there he is unjust*. . . . If you could imagine anyone obtaining this power of becoming invisible, and never doing any wrong or touching what was another's, he would be thought by the lookers-on to be a most wretched idiot, although they would praise him to one another's faces, and keep up appearances with one another from a fear that they too might suffer injustice.[3]

Of course no such rings exist, but the intrigue still persists. There is arguably no greater example of a forum where Plato's theories can be tested than today's Internet, where, as this Comment will note, anonymity is a luxury *assumedly* imbedded in the Internet's framework and fiercely defended by many individuals.[4]

Since the advent of the World Wide Web in the early 1990s, and the exponentially growing use of its vast array of networks and online communications, the Internet has proffered a collection of legal issues that courts and legislators have struggled to accommodate. At the core of many contemporary legal battles are the perplexing issues of *privacy*, *identity*, and

---

3. *Id.* at 257-59. Plato's observations here do not entirely ignore the possible observation of an all-seeing, all-knowing deity, or source of universal moral conscience. *See* Mark L. McPherran, *Platonic Religion*, *in* A COMPANION TO PLATO 252-59 (Hugh H. Benson ed., 2006) (discussing Plato's considering a "Maker-god," immortality, and a Final Judgment). Many more allegories and classical works include references to the power of invisibility. For an interesting discussion of the semiology of the Ring of Gyges, see MARC SHELL, THE ECONOMY OF LITERATURE 13, 31 (1993) (arguing that "the power of Platonic Gyges . . . is also the power of the archetypal tyrant," and that the power to "transform visibles into invisibles and invisibles into visibles . . . is associated with new economic and political forms that shattered the previous world and its culture."). This theory is especially interesting to consider in the context of this Comment because as communities shift important transactions and communications from the tangible, physical world to online, virtual frameworks, individuals with the power to cloak their identity have a substantial advantage over others.

4. This Comment touches on the moral and ethical principles of an individual's behavior under the cloak of online anonymity, but does not attempt to address Plato's theories. It is noteworthy, however, to observe the effect that the Internet has had on certain issues that society broadly recognizes as immoral. *See, e.g.*, *Net Blamed for Rise in Children Porn*, BBC NEWS (Jan. 12, 2004), http://news.bbc.co.uk/2/hi/technology/3387377.stm ("'The internet completely changed [the accessibility of child pornography]. People perhaps with a suppressed or latent interest in it have now got a mechanism. . . . *they think the internet is anonymous*.'") (emphasis added). Of course the Internet's cloak of anonymity has also provided positive, non-nefarious advantages to individuals, and this Comment does not suggest that either side's benefits outweigh the other.

anonymity.[5] The Internet seems to have developed under the general supposition that privacy and anonymity reflect "a cornerstone of our democratic society."[6] Indeed, the First Amendment provides a great deal of protection to those who wish to communicate anonymously online.[7] Nevertheless, with the widespread use of Internet services and the increasing integration of society and culture with virtual environments, the scope of online anonymity afforded to an individual has come under increased scrutiny.[8]

The development of general privacy, identity, and anonymity jurisprudence is voluminous with broad implications and consequences. This Comment primarily focuses on the contemporary understanding of these issues in the context of the Internet, and addresses the procedural obstacles presented when attempting to litigate claims against unidentified defendants. In particular, copyright owners, such as those represented by the Motion Picture Association of America (MPAA)[9] and the Record

---

5. Ken D. Kumayama, Note, *A Right to Pseudonymity*, 51 ARIZ. L. REV. 427, 437 (2009) (noting "identity does not exist but merely seems to manifest through individuals' relationships in society" (referencing an opinion espoused in ANTHONY GIDDENS, MODERNITY AND SELF-IDENTITY: SELF AND SOCIETY IN THE LATE MODERN AGE 52 (1991))). Some of the more interesting conflicts involving anonymous parties that are yet to reach the stages of formal litigation are worth noting, including the international sensation of the recent WikiLeaks scandals (*see* Glenn Kessler, *WikiLeaks's Unveiling of Secret State Department Cables Exposes U.S. Diplomacy*, WASH. POST, Nov. 29, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112802395.html), the attacks of the hacker group Anonymous on MasterCard, Visa, and HB Gary (*see* Nate Anderson, *How one Man Tracked Down Anonymous—and Paid a Heavy Price*, *in* UNMASKED (Ars Technica Kindle ed. 2011), and the hacker 'Jester' who, almost militaristically, takes down webpages maintained by WikiLeaks, Muslim Jihadist recruitment groups, and the Westboro Baptist Church (*see* JESTER'S COURT, http://th3j35t3r.wordpress.com/ (last visited Apr. 13, 2011); *see also* Anthony M. Freed, *Patriot Hacker the Jester's Libyan Psyops Campaign*, INFOSEC ISLAND (Mar. 30, 2011), https://www.infosecisland.com/blogview/12745-Patriot-Hacker-The-Jesters-Libyan-Psyops-Campaign.html, 2011 (providing an overview of the Jester's activities)).

6. DIGITAL ANONYMITY AND THE LAW: TENSIONS AND DIMENSIONS 1 (C. Nicoll, J.E.J. Prins & M.J.M. van Dellen eds., 2003) [hereinafter DIGITAL ANONYMITY].

7. *See* JONATHAN D. HART, INTERNET LAW: A FIELD GUIDE 33-42 (5th ed. 2007).

8. *Id.*

9. The MPAA represents the six major movie studios, including Walt Disney, Paramount, Sony Pictures, Twentieth Century Fox, Universal City, and Warner Brothers. *FAQ*, MOTION PICTURE ASSOCIATION OF AMERICA, http://www.mpaa.org/faq (last visited Apr. 18, 2011).

Industry Association of America (RIAA),[10] often face the preliminary hurdle of discovering and unveiling the identity of copyright infringers, a process that frequently cripples and ends the litigation process before the merits of the claim are even considered.[11] These complications arise in large part due to an irresolute body of jurisprudence addressing a First Amendment right to anonymity on the Internet.[12] Although certain unlawful activities, such as copyright infringement, libel, and defamation, are categorically considered outside the scope of First Amendment privacy protection,[13] individuals possess legitimate privacy rights for many activities that take place on the Internet.[14] However, the degree of privacy and anonymity the law affords individuals, and what procedures establish and diminish these rights, is unclear.

---

10. Similar to the MPAA, the RIAA represents a collection of music labels and artists who "create, manufacture and/or distribute approximately 85% of all legitimate recorded music produced and sold in the United States." *Who We Are*, THE RECORD INDUSTRY ASSOCIATION OF AMERICA, http://www.riaa.com/aboutus.php (last visited April 18, 2011). The RIAA is often the named plaintiff in cases involving copyright infringement of its members' work, which is part of the RIAA "work[] to protect the intellectual property and First Amendment rights of artists and music labels; conduct consumer, industry and technical research; and monitor and review state and federal laws, regulations and policies." *Id.*

11. *See, e.g.*, Arista Records LLC v. Does 1-17, No. 6:07-CV—6197-HO (D. Or. filed Oct. 27, 2008) (moving to dismiss the case after several unsuccessful attempts to discover the identity of 17 copyright infringers at the University of Oregon). In the notorious case of *Atlantic v. Andersen*, the RIAA brought a copyright infringement suit against Anderson, a disabled single mother, for her nine-year-old daughter's illegally sharing files using Kazaa, a popular file-sharing program. No. 05-933-AS (D. Or. filed Dec. 13, 2006). The case was dismissed when the error was discovered, and Anderson filed a countersuit against the RIAA for racketeering, fraud, and deceptive business practices. *See* Eric Bangeman, *RIAA throws in the towel in Atlantic v. Anderson*, ARS TECHNICA (June 4, 2007), http://arstechnica.com/tech-policy/news/2007/06/riaa-throws-in-the-towel-in-atlantic-v-andersen.ars (discussing *Atlantic v. Andersen* and other similar cases).

12. *See* Ray Beckerman, *How the RIAA Litigation Process Works*, (Apr. 9, 2008) (unpublished article) (on file with author) *available at* http://beckermanlegal.com/pdf/?file=/howriaa.htm (discussing and summarizing several cases where various courts have come to different conclusions on what degree of privacy is afforded to individuals and what legal procedures must be taken to ascertain the real identity).

13. *See* Doe I v. Individuals, 561 F. Supp. 2d 249, 253 (D. Conn. 2008) (noting that "[t]he United States Supreme Court has . . . made clear that the First Amendment's protection extends to speech on the internet," but that this freedom "is not absolute and does not protect speech that otherwise would be unprotected." (citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 353 (1995)).

14. *Id.*

Part II of this Comment discusses the understanding of anonymity that has developed due to the structure of the Internet and the resulting legislation and litigation. Part III introduces and outlines the case of *Arista Records v. Does 1-16* to date.[15] Part IV suggests that the procedural accommodation of an individual's anonymity be reconsidered, and proposes a framework to determine who mediates the disclosure of an individual's identity on the Internet. Finally, this Comment suggests that current legislation addressing copyright infringement should be amended to accommodate new technological procedures, or courts should adopt a broad reading that permits lawful subpoena power when the defendant is anonymous.

II. BACKGROUND

In many cases involving disputes over online conduct, parties bringing suit against unknown defendants, known as "John Does," encounter procedural complications at the outset of the litigation.[16] In such cases, the defendant may only be known by the numerical identifier assigned to him by his Internet Service Provider (ISP), and translating this number into a name can only be accomplished with the assistance of the ISP, which most often requires a court order.[17] Attaining such an order, however, is often

---

15. After this Comment was completed and accepted for publication, the District Court for the District of Columbia released an opinion that has gained considerable publicity and has been cautioned as "what may be the most important decision to date in the ongoing mass-litigation campaign against thousands of individuals who traded copyrighted movies on BitTorrent." Eriq Gardner, *Mass-Suing of Pirates Gets Shot In Arm Thanks to DC Judge*, THE HOLLYWOOD REPORTER (Mar. 23, 2011, 10:44 AM), http://www.hollywoodreporter.com/thr-esq/mass-suing-pirates-gets-shot-170403 (reporting on Call of the Wild Movie, LLC v. Does 1-1,062, No. CIV.A. 10-455 BAH, 2011 WL 996786 (D.D.C. Mar. 22, 2011)). Addressing Motions to Quash or Modify subpoenas that were issued in three separate, pending copyright infringement cases, Judge Beryl A. Howell issued a memorandum opinion that opponents interpreted as "waiv[ing] away procedural objections, jurisdictional concerns, and First Amendment arguments and will allow several film production companies to pursue what some have termed the 'mass-suing' of alleged pirates." *Id*. While the author of this Comment does not agree with the court's ultimate conclusion, this case addressed principles of Internet anonymity and privacy that, unfortunately, substantiate the underlying premise of this Comment. Accordingly, this Comment addresses Judge Howell's opinion at relevant sections, and for purposes of academic debate, sides with many of the legal conclusions found in *Call of the Wild*.

16. *See infra* Part III.

17. *See Call of the Wild*, 2011 WL 996786 at *14 (noting that "Amici and Time Warner do not dispute that the plaintiffs have no other sources for the information they seek.").

denied on procedural and policy grounds.[18] As this Comment argues, these difficulties are in part due to legislators' and courts' failure to react to the rapidly developing and adjusting Internet by providing procedural safeguards for end-users, ISPs, and plaintiffs seeking relief.

A. The Architecture of the Internet and the Debate over Anonymity

The Internet is an international system of networked computers.[19] There are many different types of computer networks, but, in the most general and basic sense, these networks consist of "two or more computers connected by some means through which they are capable of sharing information."[20] Relying on the Internet Protocol Suite, computers are assigned numerical Internet Protocol (IP) addresses that identify their location on networks.[21] For the majority of consumers, these IP addresses are assigned by their ISP.[22] For students on university or college campuses, local administrators oversee network access and assign IP addresses to connected computers.[23] These IP addresses become the sole virtual identity linking online activity with the physical computer and thereby its user.[24] Accordingly, users first

---

18. *See* Kumayama, *supra* note 5, at 430-37.

19. Chris Nicoll, *Concealing and Revealing Identity on the Internet*, *in* DIGITAL ANONYMITY, *supra* note 6, at 102.

20. GARY A. DONAHUE, NETWORK WARRIOR 3 (2007).

21. JOHN BLOOMER, POWER PROGRAMMING WITH RPC 105-07 (1992); ROBERT JONES, INTERNET FORENSICS 11 (2005).

22. There are many ISPs in the United States, with five of the largest including AT&T, Comcast, Road Runner, Verizon, and America Online. *Top 23 U.S. ISPs by Subscriber: Q3 2008*, ISP PLANET, http://www.isp-planet.com/research/rankings/usa.html (last visited Apr. 18, 2011).

23. For example, here at Liberty University, the administrators limit Internet access by requiring all computers to install software that identifies the computer as linked to a student or faculty identity and account. *HelpDesk Policies*, LIBERTY UNIVERSITY, https://www.liberty.edu/index.cfm?PID=17871 (last visited Apr. 18, 2011). This static link between the student's identity and his online *activities* should dismiss any supposition of anonymity, and the University makes no illusion to protecting this information from legitimate inquiring outsiders, as the "Copyright Compliance" section notes:

> Failure to adhere [to copyright compliance] is against the law and may result in the FBI as well as the RIAA coming after those in defiance. If served a subpoena, Liberty will give out names in compliance with the law. Remember that you are ultimately responsible for any uploading or downloading of files from your computer that infringe on copyright.

Id.

24. It is important to note, however, that this is a simplification of an often much-more difficult process. Matching the IP address to the real identity of the actual user is often a

accessing the Internet are known only by their IP address, and may voluntarily reveal their true identity at will or choose to remain generally incognito.[25] Individuals may choose to forgo anonymity by communicating their true identity directly to others, for instance, by voluntarily revealing identifying information on a website or by revealing financial information in commercial exchanges.[26]

Issues of involuntary disclosure tend to arise when a person has acted unlawfully and could be subject to civil liability or criminal penalties.[27]

---

difficult process, even for an ISP. The technical reasons for this are beyond the scope of this Comment, but for an explanation and in-depth discussion, *see* Nicoll, *supra* note 19, at 101-08.

25. *Id.* at 100.

26. Facebook's "Privacy Guide" page entitled "Controlling How You Share" offers an excellent example of this proposition, where the internationally popular social networking titan advises users that: "Our privacy controls give you the power to decide what and how much you share. Learn how to manage who can see your information on and off Facebook." *Controlling How You Share*, FACEBOOK, https://www.facebook.com/privacy/explanation.php (last visited Apr. 18, 2011) (providing instructions to limit what information is revealed). The popular online auction and shopping company eBay provides a forum for merchants and shoppers, where the degree of personal, identifying information is up to the user:

> Your User ID is displayed throughout eBay (and so available to the public), and is connected to all of your eBay activity. Other people can see your bids, purchases, items for sale, storefronts, feedback, ratings and associated comments. Notices sent to other community members about suspicious activity and policy violations on our sites refer to User IDs and specific items. So if you associate your name with your User ID, the people to whom you have revealed your name will be able to personally identify your eBay activities.

Summary of Our Privacy Policies, EBAY, http://pages.ebay.com/help/policies/privacy-policy.html#Activity (last visited Apr. 18, 2011). An interesting observation here and in services similar to eBay is that *pure* anonymity is rarely afforded, and the *limited* anonymity afforded proves contradictory because transactions are preferred with known identities. Individuals operate under the guise of *pseudonymity*, where the "User ID" embodies an identity where the "character" of that person is determined by their transactional history. PayPal, the popular e-commerce tool advertising itself as "PayPal. Privacy built in," provides users with an option to engage in online financial transactions without revealing banking or credit card information. *Shop Without Sharing*, PAYPAL, https://www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing/general/Shopwoutshare-outside (last visited Apr. 18, 2011).

27. It should be noted that connecting an IP address with an Internet subscriber's true identity is not an easy, automated task. Rather, it places a significant burden on ISPs who have limited resources and must prioritize compliance requests, first serving urgent law enforcement inquiries such as "suicide threats, child abduction cases, and terrorist activity." Nate Anderson, *Turning Numbers into Names: How IP Address Lookups Are Done*, ARS

Although some may consider the Internet, or niche corners of the Internet, to be a modern-day Wild West where the law is so vague as to be either exploitable against the weak or ignored altogether, this is not the case.[28] The many activities, communications, and interactions that take place within a "virtual" environment are still subject to state, federal, and even international laws.[29] Accordingly, although anonymity may be expected and granted for many online activities, society must retain procedural methods to determine the real identities of wrongdoers.[30] The question of anonymity is therefore necessarily a matter of degree, and there is no consensus as to this balance.[31]

Proponents of anonymity note the openness that accompanies the ability to communicate without the insecurities that often plague people.[32] Proponents argue that anonymous communication allows a "digital personae," which is liberating and has the effect of increasing the quantity and quality of discourse and collaboration.[33] A likely result, they contend, is that discourse "must be judged solely on the[] content as there is literally nothing else to go by."[34] The obvious argument against this is that it also

---

TECHNICA (Feb. 1, 2011, 6:50 AM), http://arstechnica.com/tech-policy/news/2011/02/how-internet-providers-look-up-an-ip-address.ars.

28. *See* Lyombe Eko, *American Exceptionalism, the French Exception, Intellectual Property, and Peer-to-Peer File Sharing on the Internet*, 10 J. MARSHALL REV. INTELL. PROP. L. 95, 130-34 (2010) (describing "Peer-to-Peer Exchanges as the Wild West of American Intellectual Property Enforcement").

29. *See, e.g.*, 17 U.S.C. § 512 (2010) (providing a safe harbor from liability to ISPs for copyright infringing materials passing through the ISPs network); 18 U.S.C. § 1030(a)(3) (2010) (criminalizing trespassing in a federal computer); Seidl v. Greentree Mortg. Co., 30 F. Supp. 2d 1292 (D. Colo. 1998) (denying attorney's claim of absolute immunity for potentially libelous statements posted on a website); Andrew S. Kaufman & Betsey D. Baydala, *Redress Cyberbullying as an Intentional Infliction of Emotional Distress*, N.Y. L.J. (Feb. 11, 2011), *available at* http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202481607795 (addressing the viability of trying "cyberbullying" claims under the tort of intentional infliction of emotional distress); European Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (acknowledging the right to privacy and the need to protect personal information from unwanted access and use).

30. *See* Nicoll, *supra* note 19, at 100.

31. DIGITAL ANONYMITY, *supra* note 6, at 6.

32. *Id.* at 7.

33. *Id.* at 8. Of course, this "digital personae" falls within the paradigm of pseudonymity and does not provide *pure* anonymity. *See supra* note 26.

34. *Id.*

allows for bigotry and hateful speech to go virtually unchecked.[35] These arguments are especially prominent in cases involving defamation and libel.[36] Anonymity may also "enhance the individual's sense of privacy and insulate the speaker from unauthorized efforts to probe his persona."[37] Accordingly, some degree of privacy provides for greater online freedom to engage in discourse, disclose personal information, and speak openly without fear of retribution.[38]

Opponents of unqualified or broadly defined anonymity tend to agree with Justice Scalia's conclusion that it "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of anonymity."[39] Unaccountable use rescinds personal responsibility and permits individuals to act without fearing consequences to themselves, others, or society.[40] The same degree of freedom that permits individuals to feel comfortable revealing personal information may also empower individuals to communicate lies, lambast others with hateful speech, or transmit unlawful content. Accordingly, it is not surprising that claims for anonymous protection often arise as a defense.[41] Because the right to anonymity is presumed as a *privacy* issue, would-be defendants are hedged behind the additional burden placed on the plaintiff to show cause before the law

---

35. *See* McIntyre v. Ohio Election Comm'n, 514 U.S. 334, 385 (1995) (Scalia, J., dissenting) (rejecting the majority's "perception that 'anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.'") (citations omitted). Justice Scalia concluded: "I can imagine no reason why an anonymous leaflet is any more honorable, as a general matter, than an anonymous phone call or an anonymous letter. *It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity*." *Id.* (emphasis added).

36. *See, e.g.*, Doe v. 2TheMart.com, 140 F. Supp. 2d 1088 (W.D. Wash. 2001); Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. Super. Ct. App. Div. 2001); Melvin v. Doe, 836 A.2d 42 (Pa. 2003).

37. MADELEINE SCHACHTER & JOEL KURTZBERG, LAW OF INTERNET SPEECH 428-29 (3d ed. 2008).

38. *Id.* at 429.

39. DIGITAL ANONYMITY, *supra* note 6, at 7 (quoting *McIntyre*, 514 U.S. at 385).

40. *Id.* ("Anonymous communication is a great tool for evading detection of many varieties of illegal and immoral activity.").

41. *See, e.g.*, Dendrite Int'l, Inc. v. Doe 775 A.2d 756 (N.J. 2001) (seeking to identify a person who posted defamatory material on an Internet bulletin board); O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006) (alleging that several anonymous defendants leaked confidential information about new Apple Computer products to several websites before Apple released the products).

permits forced disclosure of the anonymous defendant's real identity.[42] Because of the structure of the Internet, however, ISPs often find themselves in the middle of legal battles as a virtual citadel defending their veiled subscribers.[43]

B. Copyright Infringement and the Internet

Anonymity is a key preliminary issue in many types of civil legal actions.[44] In suits for libel and defamation, malicious "hacking," fraudulent commercial transactions, and intellectual property infringement, litigants are often forced to hurdle the identity issue and discover *who* they wish to sue, before reaching the substantive legal cause of action.[45] Of the variety

---

42. *See, e.g.*, Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578-79 (N.D. Cal. 1999). In *Columbia,* the court required the plaintiff to overcome the privilege of anonymity by demonstrating a prima facie claim, met only by satisfying three requirements:

> First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity . . . .
>
> . . . .
>
> Second, the party should identify all previous steps taken to locate the elusive defendant . . . .
>
> Third, the plaintiff should establish to the Court's satisfaction that plaintiff's suit against the defendant could withstand a motion to dismiss.

Id. See also Doe v. Cahill, 884 A.2d 451 (Del. 2005) (requiring the plaintiff to satisfy the "summary judgment" standard before obtaining the identity of an anonymous defendant in a defamation case); Best Western Int'l, Inc. v. Doe, No. CV-06-1537, 2006 U.S. Dist. LEXIS 56014 (D. Ariz. July 25, 2006) (permitting the plaintiff to discover the identities of individuals who posted comments disparaging Best Western on a website after "considerable litigation").

43. Actions brought directly against ISPs are rarely successful unless the ISP has engaged in unlawful activity itself. *See Seescandy.com*, 185 F.R.D. at 578 n.1 (noting the nature and liability of ISPs, and the difficulty of lawsuits against ISPs for their user's activities). For an interesting analysis of the different treatment ISPs receive in the United States versus other countries, see Seagull H. Song, *A Comparative Copyright Analysis of ISP Liability in China Versus the United States and Europe*, 27 THE COMPUTER & INTERNET LAW 7 (July 2010), *available at* http://works.bepress.com/seagull_song/2. *See also* Matthew Lasar, *ISPs Don't Want to be Big Content's "Judges, Juries, and Executioners,"* ARS TECHNICA (Mar. 16, 2011, 10:45 AM), http://arstechnica.com/tech-policy/news/2011/03/aussie-dsl-service-time-to-get-isps-out-of-copyright-enforcement.ars (discussing a proposal from iiNet, an Australian ISP, promoting "an alternative to the ISP-as-enforcer model" by establishing an independent third party to determine whether evidence provided by the plaintiff meets the legal standard before requesting the user's account information).

44. DIGITAL ANONYMITY, *supra* note 6, at 1.

45. *See supra* note 42. Interestingly, the defendant is not always the only anonymous party to a lawsuit. For example, in *America Online, Inc. v. Anonymous Publicly Traded Co.*

of claims, cases for copyright infringement resulting from unauthorized file-sharing has gained considerable notoriety in recent years, due in part to the popularity of music and video file-sharing.[46] These cases usually involve some form of sharing copyrighted materials, such as music, videos, or software, without the express authorization of the copyright owner, which is a direct infringement of the owner's copyrights.[47] With more than 2.6 billion files being illegally shared per month, copyright owners' concerns for protecting their property is understandable.[48] While some derisively characterize the unauthorized sharing of copyrighted content as "piracy,"[49] others view such sharing as ethical and "an act of respect."[50]

---

an anonymous plaintiff sought a *subpoena duces tecum* requiring the ISP to disclose the identities of anonymous John Doe defendants who allegedly defamed and shared confidential information in Internet chat rooms. *In re* Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26 (Va. Cir. Ct. 2000), *rev'd sub nom* America Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001). AOL, the ISP to several of the defendants, moved to squash the subpoena, but the trial court refused the motion. AOL appealed, and the Virginia Supreme Court reversed, requiring the anonymous plaintiff to reveal his or her identity before continuing with the case. Anonymity is not only an issue in civil cases, but also poses hurdles in criminal cases. *See also* Indira Carr, *Anonymity, the Internet and Criminal Law Issues*, *in* DIGITAL ANONYMITY, *supra* note 6, at 189-97 (noting the problems UK law enforcement face when gathering evidence for prosecution of criminal acts such as child pornography).

46. HART, *supra* note 7, at 233.

47. *See* 17 U.S.C. § 102 (2010) (affording copyright protection to "original works of authorship fixed in any tangible medium of expression"); 17 U.S.C. § 1201 (2010) (extending copyright protection to cover digital work, and prohibiting circumvention of digital copyright protection technologies).

48. *Music United for Strong Internet Copyright, Online Music Sharing is Wrong*, *reprinted in* INTERNET PIRACY 8 (James D. Torr, ed., Thomson Gale 2005).

49. "Some" may be an understatement, considering the FBI has adopted the term. *Anti-Piracy Warning Seal*, FBI, *available at* http://www.fbi.gov/about-us/investigate/cyber/ipr/anti-piracy (last visited Apr. 18, 2011). *See also* HART, *supra* note 7, at 263 (noting that in March 2004, Congress introduced, but failed to pass, a bill entitled The Protecting Intellectual Rights Against Theft and Expropriation Act of 2004 (the "PIRATE Act"), S. 2237, 108th Cong. (2004)) (permitting "the Department of Justice to bring a civil action against suspected copyright infringers"). The file-sharing community has also proudly claimed the 'pirate' epithet. *See, e.g.*, THE PIRATE BAY, http://thepiratebay.org/ (last visited Apr. 18, 2011). The Pirate Bay is a file-sharing site started and maintained by a Swedish anti-copyright organization. As an interesting side note, not everyone views the act of pirating copyrighted material as wrong. *See* Anthony G. Gorry, *Many People Do Not View Online Music Sharing as Wrong*, *reprinted in* INTERNET PIRACY, *supra* note 48, at 22.

50. *See* Enigmax, *File-Sharers Await Official Recognition of New Religion*, TORRENT FREAK (Apr. 18, 2011), http://torrentfreak.com/file-sharers-await-official-recognition-of-new-religion-110410/.

Accordingly, for those opposed to file-sharing, Internet piracy is viewed as a dangerous and destructive activity, while proponents of file-sharing celebrate it as beneficial to the artistic community at large.[51]

The merits of the various policy arguments on either side of the debate are beyond the scope of this Comment. There is generally no dispute over whether a copyright is infringed when an individual shares or receives unauthorized copyrighted material from another person in the United States.[52] The Copyright Act of 1976 provides protected ownership rights to "original works of authorship fixed in any tangible medium of expression."[53] This protection is as applicable to digital works as it is to physical works.[54] However, U.S. copyright protection only extends so far. The transnational nature of the Internet exposes artists' work to foreign countries and laws, and opens the door for a vast array of opinions and arguments regarding the use and nature of shared content.[55] As one author notes, while copyright law is well developed in the United States, "nine-tenths of the people on the planet are from cultures or political systems that don't have a concept of or laws regarding intellectual property—in fact, many don't recognize individual property ownership."[56] This fact may account for the diversity of ideologies surrounding the file-sharing debate, but it does not negate or address the simple fact that many people own

---

51. *See* Bonnie J.K. Richardson, *The Government Must Combat Online Piracy*, *reprinted in* INTERNET PIRACY, *supra* note 48, at 49 (testifying before the House Subcommittee on Commerce, Trade, and Consumer Protection that "Internet piracy is the single biggest impediment to digital trade today."). *But see* Hal Plotkin, *Online File Sharing Will Benefit Society*, *reprinted in* INTERNET PIRACY, *supra* note 48, at 66 (envisioning the positive transformation of "a new, sharing world").

52. Copyright infringement is in no way confined within the boundaries of the United States. The International Intellectual Property Alliance, a "private sector coalition [of trade associations] represent the U.S. copy-right based industries," in a recent report to the Office of U.S. Trade Representatives noted that "[t]heft of U.S. [c]reative [c]ontent is a [g]lobal [p]roblem." Letter from Eric H. Smith, Int'l Intellectual Prop. Alliance, to Stanford McCoy, Assistant U.S. Trade Representative for Int'l Prop. and Innovation (Feb. 17, 2009), *available at* http://www.iipa.com/2009_SPEC301_TOC.htm (follow "IIPA's Eric H. Smith Letter to Stan McCoy, Assistant United States Trade Representative") (last visited May 1, 2011). *See also International Intellectual Property Alliance 2011 Special 301 Report*, INT'L INTELLECTUAL PROP. ALLIANCE, http://www.iipa.com/2011_SPEC301_TOC.htm (last visited May 1, 2011) (listing countries in order of priority for copyright violating activities).

53. 17 U.S.C. § 102 (2010).

54. *See* 17 U.S.C. § 506(a)(1)(C) (2000).

55. *See International Intellectual Property Alliance*, *supra* note 52.

56. JOHN GANTZ & JACK B. ROCHESTER, PIRATES OF THE DIGITAL MILLENNIUM 5 (Financial Times Prentice Hall 2005).

copyrights and intellectual property that are unlawfully shared across the Internet.[57]

People share media over the Internet through various file-sharing methods, including "hosted" and "peer-to-peer" (P2P) protocols.[58] While the content shared across these networks remains the same, the methods of storing, serving, and sharing the content have several unique legal implications.[59] There is an important distinction between "hosted" and "P2P" file-sharing. Hosted file-sharing involves a centralized server where files are stored and available for download and distribution.[60] The popular file-sharing software Napster operated as a hosted file-sharing network prior to its legal challenges,[61] and it continues to operate as a legitimate form of centralized file-sharing today.[62] The shutdown of Napster, while a

---

57. MITCH BAINWOL, THE MUSIC INDUSTRY'S LAWSUITS AGAINST ONLINE MUSIC SHARERS ARE JUSTIFIED (2003), *reprinted in* INTERNET PIRACY 52 (James D. Torr, ed., Thomson Gale 2005).

58. Peer-to-peer file-sharing is a somewhat technically complicated procedure, but has been defined as where "the participants share a part of their own hardware resources (processing power, storage capacity, network link capacity, printers). These shared resources are necessary to provide the Service and content offered by the network (e.g. file-sharing or shared workspaces for collaboration). They are accessible by other peers." *Glossary of Peer-to-Peer Terminology*, P2P NETWORKING AND APPLICATIONS, http://www.p2pna.com/glossary.html (last visited Apr. 8, 2011). *See also* GANTZ, *supra* note 56, at 179-82 (providing "An Anatomy of Downloading" through the popular KaZaA protocol).

59. As the culture of file-sharing continues to develop, so does the method of sharing. Hosted file-sharing was popular prior to the takedown of Napster, and P2P rose to take its place. However, now that P2P has fallen under close scrutiny, Usenet, a form of centralized, hosted file-sharing, and "direct http" downloads from "file lockers" are becoming more popular in the file-sharing culture. *See How to Use Usenet, a Beginners Guide*, TORRENTFREAK (Apr. 4, 2007), http://torrentfreak.com/how-to-use-usenet-a-beginners-guide; TEHPARADOX.COM, http://tehparadox.com/ (last visited May 1, 2011) (providing users with forums to share links to files on paid servers known as "file lockers" such as http://www.fileserve.com and http://www.megaupload).

60. *See, e.g.*, MEGAUPLOAD, http://www.megaupload.com (last visited May 1, 2011); RAPIDSHARE, http://www.rapidshare.com (last visited May 1, 2011); FILESERVE, http://www.fileserve.com (last visited May 1, 2011).

61. *See* A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (2000). The RIAA filed suit against Napster for contributory and vicarious copyright infringement and was awarded an injunction against Napster, enjoining Napster from "engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of the rights owner." *Id.* at 927.

62. ANDREW A. ADAMS & RACHEL MCCRINDLE, PANDORA'S BOX: SOCIAL AND PROFESSIONAL ISSUES OF THE INFORMATION AGE 433 (2008).

victory for copyright owners, forced the Internet culture to adopt a decentralized form of file-sharing in an attempt to avoid legal complications.[63] P2P file-sharing succeeded as a plausible alternative to centralized file-sharing and has proven more complicated and difficult to litigate—as this type of technology allows users to connect directly to each other without a mediating third party vulnerable to DMCA takedown regulations.[64] Among the many forms of P2P communication protocols, BitTorrent is arguably the most popular, and has been the subject of several highly publicized copyright infringement cases.[65]

C. Congress's Response to Developing Technologies: The Digital Millennium Copyright Act

In response to the copyright issues arising as result of the emerging popularity of file-sharing, Congress enacted the Digital Millennium Copyright Act (DMCA) in 1998.[66] This Act effectively ratified two treaties of the World Intellectual Property Organization,[67] criminalizing the development and use of technologies commonly used to pirate copyrighted works and, at the same time, limiting the liability of service providers.[68]

---

63. *See* Emily Elias, *BitTorrent Keeps File-Sharing Going Strong*, STRAIGHT.COM (Jan. 27, 2011), http://www.straight.com/article-370564/vancouver/bittorrent-keeps-filesharing-going-strong ("With any file-sharing site you try to shut down, a new file-sharing site is bound to pop up, and that has happened in the past—with Napster, then Kazaa. . . . There is no way you can shut file-sharing down.").

64. This is a matter of technicality, as the ISP is still the one providing access to the Internet.

65. The BitTorrent P2P protocol is especially useful in distributing and transferring larger files across the Internet. *What is BitTorrent?*, BITTORRENT, http://www.bittorrent.com/btusers/what-is-bittorrent (last visited May 1, 2011).

66. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.).

67. *WIPO*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/wipo (last visited May 1, 2011) ("The World Intellectual Property Organization (WIPO) is the UN agency responsible for treaties involving copyright, patent, and trademark laws."). While WIPO was key in laying ground for international intellectual property policy, other groups, such as the Trans-Pacific Partnership, continue to push for the expansion of trade agreements addressing copyright protection. *See* Nate Anderson, *Son of ACTA: Meet the* Next *Secret Copyright Treaty*, ARS TECHNICA (Mar. 11, 2011 11:20 AM), http://arstechnica.com/tech-policy/news/2011/03/son-of-acta-meet-the-next-secret-copyright-treaty.ars (discussing the "Trans-Pacific Partnership," and the "secret" intellectual property chapter drafted by the United States that was leaked on March 10, 2011 and quoting Michael Gist, Canadian law professor, describing the chapter as "everything [the US] wanted in ACTA but didn't get.").

68. H.R. REP. No. 105-551(I), at 9 (1998).

The DMCA acknowledged the unique relationship an ISP has with both its customers and copyright owners whose property may be transmitted through its systems and networks.[69] In essence, Congress was acknowledging the unprecedented role that ISPs play in providing a unique service to individuals. One of the key measures the DMCA adopted was to differentiate between "direct infringement" and "secondary liability."[70] Direct infringement is assessed against those principally involved in the copyright infringing activity, while secondary liability attaches to "passive, automatic acts engaged in through a technological process initiated by another."[71] By creating this dichotomy, Congress intended to encourage cooperation between those attempting to enforce their copyright and those in the position to "prevent ongoing infringement."[72]

Despite the thorough scope of the DMCA and the considerable number of amendments,[73] several of its inherent flaws create severe enforcement difficulties. The DMCA is weakened by two key errors: first, the DMCA overextends ISP immunity and fails to provide adequate measures for subpoena process;[74] and second, the DMCA fails to address and define requisite boundaries for anonymity and identification of end-users. Together, these missteps limit the applicability of the DMCA by failing to provide an adequate process for copyright owners to identify a substantial class of purported infringers.

The DMCA's broad exemption of ISP liability and the limitation on subpoena power severely misunderstands the structure and nature of ISP-end user relationships. Title II of the DMCA affords ISPs immunity from

---

69. *Id*. at 11.

70. *Id*.

71. *Id*.

72. Katherine Raynolds, Comment, *Note: One Verizon, Two Verizon, Three Verizon, More?—A Comment: RIAA v. Verizon and How the DMCA Subpoena Power Became Powerless*, 23 CARDOZO ARTS & ENT L.J. 343, 349 (2005).

73. The Act has been amended thirty-two times since its creation. *See* 7 MELVILLE B. NIMMER AND DAVID NIMMER, NIMMER ON COPYRIGHT App. 2-1 (Matthew Bender rev. ed., 2009).

74. This Comment does not suggest that the subpoena power should be more lenient to litigants, but rather that the procedures are inadequately defined and based on outdated policy considerations, at one time providing litigants an opportunity to misue the DMCA to gain easy access to defendants while ultimately becoming useless. *See No Downtime for Free Speech Campaign*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/ip-and-free-speech (last visited July 2, 2011); Reynolds, *supra* note 72, at 349.

monetary and injunctive relief under four explicit conditions.[75] First, ISPs cannot be liable for "transmitting, routing, or providing connections for material through a system or network controlled or operated by or for the service provider" so long as the material meets a set of criteria and, upon notice, "the ISP follows certain 'notice and take down' procedures."[76] Second, the "intermediate and temporary storage" of copyrighted material does not create ISP liability per se.[77] Third, even material residing on the ISP's system or controlled network will not create liability so long as the ISP lacked knowledge of it and received no financial benefit from it.[78] Finally, an ISP will not be liable for "referring or linking" to infringing material through "information location tools, including a directory, index, reference, pointer, or hypertext link."[79] A key characteristic of all of these exemptions is that the ISP does not actively promote the unlawful activity, and upon notice of such activity, takes active steps to stop the infringement.

Once the infringing activity is recognized, a copyright owner may subpoena the ISP to identify the user.[80] Often a third party will monitor a shared file, harvesting and recording the IP address of those participating in the "swarm" as each connected user can see the IP address of others.[81] Attorneys representing copyright holders will then present the list of IP addresses to a court in the complaint and seek to discover the associated identities from the ISP.[82] This is the procedure that has come under the

---

75. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1234 (D.C. Cir. 2003).

76. Raynolds, *supra* note 72, at 349. *See also* 17 U.S.C. § 512(c)(1)(C) (2000). In general, the ISP must play a passive role and cannot store information on its hardware.

77. 17 U.S.C. § 512(b) (2000).

78. 17 U.S.C. § 512(c) (2000).

79. 17 U.S.C. § 512(d) (2000).

80. Nate Anderson, *Turning Numbers into Names: How IP Addresses Lookups Are Done*, ARS TECHNICA (Feb. 1, 2011, 6:50 AM) (describing the subpoena process in Achte/Neunte Boll Kino Beteiligungs Gmbh & Co. v. Does 1-4,577, 736 F. Supp. 2d 212, 213 (D.D.C. 2010)).

81. Enigmax, *Hustler Hires Media Protector to Chase Online Porn Pirates*, TORRENTFREAK (Jan. 3, 2009), http://torrentfreak.com/hustler-hires-media-protector-to-chase-porn-pirates-090103/. As an example of this type of information gathering, in *Call of the Wild* the plaintiffs enlisted Guardaley Limited, "an anti-piracy firm that uses proprietary technology to identify BitTorrent users sharing the plaintiff's copyrighted works." Call of the Wild Movie, LLC v. Does 1-1,062, CIV.A. 10-455 BAH, 2011 WL 996786 (D.D.C. Mar. 22, 2011).

82. For an excellent example of a list of IP addresses presented to a court, see Exhibit C to Motion for Leave for Discovery (Hurt Locker), Voltage Pictures, LLC v. Does 1 – 5,000,

greatest degree of scrutiny and where much of the controversy begins. Section 512(h) of the DMCA provides the copyright owner with the subpoena power necessary to identify the infringer, so long as he provides the information listed under subsection (c)(3)(A).[83] Although the language in this section is clear, simple, and straightforward, the demand for the requisite information of the infringing user has raised serious privacy concerns.[84] In theory, the DMCA allows a copyright owner to discover the identity of an individual with only a preliminary prima facie showing of a potential legal cause.[85] However, it may be the case that the language is *so* simple that it has crippled the effectiveness of the DMCA.

Although one of the primary purposes of the DMCA is to provide copyright owners with procedures to protect their property by identifying purported infringers, the DMCA offers very little guidance for determining when subpoenas should be granted.[86] Congress has ultimately left this decision to the courts, and a variety of inquiries and tests have been established attempting to ascertain when an ISP falls under the purview of the DMCA.[87] This is a somewhat technical undertaking and requires an understanding of ISP's technical functions and their relationships with subscribers.

In the hallmark DMCA case of *RIAA v. Verizon*, the Second Circuit noted the inherent failure of the DMCA to accommodate the popular P2P file-sharing technology.[88] Here, the RIAA believed a subscriber of the ISP Verizon was engaging in copyright infringement by sharing music through

---

Civ. A. No. 1:10-cv-00873-RMU, *available at* http://www.scribd.com/doc/32726320/Volt-Pict-2573095-3-3943 (last visited May 1, 2003).

83. 17 U.S.C. §§ 512(h), (c)(3)(A) (2000) (requiring that the copyright owner, along with his own contact information and proof of copyright ownership, must provide, "Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material").

84. Patrick Fogarty, *Major Record Labels and the RIAA: Dinosaurs in a Digital Age?*, 9 HOUS. BUS. & TAX L.J. 140, 152 (2008).

85. *Id*.

86. 17 U.S.C. § 512(c)(3)(A)(iii) (2000) (requiring "information reasonably sufficient to permit the service provider to locate the material" but not providing any further guidelines and leaving what constitutes "information reasonably sufficient" to the discretion of the clerk).

87. *See, e.g.*, Fogarty, *supra* note 84, at 154 (discussing several factors courts have determined when granting subpoenas).

88. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1234 (D.C. Cir. 2003).

a P2P program, and served Verizon with a subpoena seeking to identify the purported infringer.[89] Verizon refused, and the District Court granted the RIAA's motion to compel discovery.[90] Verizon appealed, and the Second Circuit reversed, noting that the "information" required for the subpoena must indicate activity described under § 512(a)–(d).[91] The Second Circuit interpreted this to mean that the subpoena power is "structurally linked to the storage function of an ISP, not the transmission function."[92] Additionally, the Second Circuit noted that the legislative history of the DMCA indicated that Congress was unaware that users would be able to "directly . . . exchange files containing copyrighted works."[93] In fact, this has become a "widely popular" form of sharing for both music and video files.[94] Consequently, the DMCA is inapplicable when users directly interact with one another and the ISP is passive and merely providing access to the networks over which it has little or no control.[95]

D. Case in Point: RIAA and John Doe Litigation

After a series of futile DMCA litigation attempts,[96] the RIAA began initiating John Doe lawsuits.[97] In these cases, the RIAA files a complaint identifying the anonymous defendants only by their "numerical IP address."[98] The RIAA then files *ex parte* expedited discovery requests to

89. *Id.* at 1231.

90. *Id.*

91. *See supra* note 79 and accompanying text.

92. Fogarty, *supra* note 84, at 154 (citing *Verizon*, 351 F.3d at 1237).

93. *Verizon*, 351 F.3d at 1238.

94. *See* HART, *supra* note 7, at 233.

95. *See, e.g.*, *Verizon*, 351 F.3d 1229 (holding that the DMCA only permits the issuance of subpoenas when an ISP engages in hosting copyright infringing materials on its servers, and the not when the ISP is "acting *as a conduit* for P2P file-sharing") (emphasis added); *In re* Charter Commc'ns, Inc., 393 F.3d 771 (8th Cir. 2005); *In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005) (applying the same "act[ing] as a conduit" rationale in determining that the DMCA does not apply to universities acting as ISPs).

96. *See, e.g.*, *Verizon*, 351 F.3d 1229, *In re Charte*r, 393 F.3d 771; *In re Subpoena to University of North Carolina*, 367 F. Supp 2d 945.

97. Fogarty, *supra* note 84, at 156.

98. *Id*.

subpoena the ISP "to determine the true identities of Doe Defendants."[99] If the court grants the request, the ISP is served with the subpoena demanding disclosure of "the name, current (and permanent) addresses and telephone numbers, email addresses, and Media Access Control for each Defendant."[100] At this point the ISP may then communicate a letter to the Does "indicating that an order has already been granted against them."[101] If and when the subpoena provides the names and addresses of the subscribers, the RIAA will drop the John Doe case and file a new suit against the defendant in his real name.[102]

---

99. *See, e.g.*, Ex Parte Application For Leave to Take Immediate Discovery at 2, Arista Records LLC v. Does 1-22, No 8 Civ. 00066-S-DLM (D. R.I. filed Feb. 27, 2008) *available at* http://www.ilrweb.com/viewILRPDF.asp?filename=arista_does1-22_080228Motion.

100. *Id.* Fogarty, *supra* note 84, at 156 (noting that these have been routinely granted). MAC addresses are unique identifiers assigned to most network adapters or network interface cards, consisting of both letters and numbers. PAWAN K. BHARDWAJ, A+, NETWORK+, SECURITY+ EXAMS IN A NUTSHELL: A DESKTOP QUICK REFERENCE (2007). There are three key differences between IP addresses and MAC address that make MAC addresses less reliable for the purposes of identification. First, MAC addresses are usually encoded in the physical hardware of a device, while the ISP assigns IP addresses to the end-users. DANIEL STEINBERG AND STUART CHESHIRE, ZERO CONFIGURATION NETWORKING: THE DEFINITIVE GUIDE 24 (2005). The benefit of the MAC address is that it will remain the same even if the user uses different service providers. For example, if an individual accesses the Internet at a café offering WiFi, and hours later returns home and uses his personal WiFi there, his MAC address will remain the same, while his IP address will have changed. Second, although this is intended to be a permanent assignment, it is possible to change the MAC address—known as "spoofing" the address. ANDREW LOCKHART, NETWORK SECURITY HACKS 67 (2004); MATTHEW GAST, 802.11 WIRELESS NETWORKS: THE DEFINITIVE GUIDE 480 (2d, 2005). Therefore, while the assignment of the static MAC address is beneficial when one moves between ISPs, it is also less-beneficial in that a knowledgeable computer user is able to continually change his MAC address at whim. Finally, MAC addresses are difficult to track geographically as they will only reveal the identity of the manufacturer and hardware device, while IP addresses *may* provide more information as to the location of the device on the network itself.

101. Beckerman, *supra* note 12.

102. *See also* Denise Howell, *P2P. . . You And Me*, THIS WEEK IN LAW (Apr. 26, 2009), http://www.podtrac.com/pts/redirect.mp3/twit.cachefly.net/TWiL-023.mp3 (interviewing Ray Beckerman, who is heavily involved in RIAA litigation and noting that RIAA will occasionally also add the real identity of the individual to the John Doe suit as a third party without dropping the original suit). This Comment assumes, for the sake of argument, that these are legitimate procedures that copyright owners necessarily follow in a good faith attempt to enforce their copyright, but there are strong arguments against this presumption. *See* Nate Anderson, *Judge: P2P Class-Action Suit Looks Like a "Fishing Expedition,"* ARS TECHNICA (Mar. 10, 2011 11:43 AM), http://arstechnica.com/tech-policy/news/2011/03/judge-p2p-class-action-suit-looks-like-a-fishing-expedition.ars.

A notable and controversial result of this litigation method is that for the first stages of the suit, the actual defendants are not on notice of pending litigation and are without representation.[103] This has been decried as an unlawful and unethical approach to litigate Internet copyright infringement cases.[104] Courts have looked with disfavor on this John Doe procedure, noting, "in several important ways[,] they are less protective of the rights of service providers and Internet users [than in DMCA litigation]."[105] Yet, without adequate measures to uncover the identity of infringers, the RIAA and similar copyright owners are without alternative procedures to enforce their ownership rights.

There are several additional drawbacks to John Doe litigation; the process is expensive, time-consuming, and often ends before the merits of the case are even considered.[106] While broadband-speed Internet access is beneficial for those who wish to access or share files, the length of time required to request and receive a subpoena often undermines the ability of copyright owners to prevent further infringement.[107]

III. THE PROBLEM IN FOCUS: ARISTA RECORDS V. DOES 1-16

The recent Second Circuit case of *Arista Records v. Does 1-16*[108] offers an excellent example of the issues raised in the *John Doe* genus of RIAA litigation.[109] As in similar cases,[110] a key issue from the outset was the degree of anonymity constitutionally afforded to the defendants. Here, Arista Records LLC, along with twelve other music recording and entertainment companies (collectively *Arista*), brought suit for copyright

---

103. *See* Beckerman, *supra* note 12.

104. Fogarty, *supra* note 84, at 156 (citing Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1237 (D.C. Cir. 2003)).

105. *In re* Verizon Internet Servs., 240 F. Supp. 2d 24, 40 (D.D.C. 2003) (ordering subpoena enforcement).

106. *See* Alex Salkever, *Big Music's Worst Move Yet*, BUSINESS WEEK (Jan. 27, 2004), http://www.businessweek.com/technology/content/jan2004/tc20040127_2819_tc047.htm.

107. Raynolds, *supra* note 72, at 372.

108. Arista Records LLC v. Does 1-16, 2009 WL 414060 (N.D.N.Y. 2009), *aff'd sub nom.* Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir. 2010)

109. For a collection of similar cases, see INDEX OF LITIGATION DOCUMENTS REFERRED TO IN "RECORD INDUSTRY VS. THE PEOPLE," http://beckermanlegal.com/Documents.htm (last visited Apr. 9, 2011) (containing a detailed archive of many documents relating to RIAA litigation) and RIAA V. THE PEOPLE CASE ARCHIVE, ELECTRONIC FRONTIER FOUNDATION, http://w2.eff.org/IP/P2P/riaa_archive.php (last visited Apr. 14, 2009) (indexing cases where the EFF filed amicus briefs).

110. *Id.*

infringement against sixteen anonymous defendants, known only by their IP address.[111] *Arista* claimed the Defendants violated copyright law by the "downloading and distributi[ng] of copyrighted sound recordings owned by Plaintiffs."[112] The thirteen defendants were unrelated, except for the fact that they all used the Internet services provided by the State University of New York (SUNY).[113]

After commencing the suit, Arista filed an *ex parte* motion for leave to take immediate discovery in order to identify the Doe Defendants.[114] The trial court granted the motion and issued a subpoena upon SUNY, "seeking documents, including electronically stored information, sufficient to identify each Defendant's true name, current (and permanent) addresses and telephone numbers, e-mail addresses, and Media Access Control (MAC) addresses.[115] Defendants motioned to quash the subpoena, raising three primary arguments. First, defendants claimed that Arista's complaint was "insufficient to defeat their first amendment privilege to be anonymous."[116] Second, defendants claimed that Arista's complaint was "solely predicated on illegally obtained evidence."[117] Finally, defendants argued that "[t]he joinder of all defendants in one action is improper."[118]

The defendants' first claim is of particular interest to this Comment. The right "to use the Internet . . . anonymously," they contended, is a qualified

---

111. *Id.*

112. Complaint at ¶ 18, Arista Records LLC v. Does 1-16, 2008 WL 4337339 (N.D.N.Y. 2008).

113. Memorandum of Law in Support of Motion to Quash, Arista Records LLC v. Does 1-16, 2008 WL 5368436 (N.D.N.Y. 2008) (No. 1:08-cv-00765-NPM RFT).

114. Brief of Plaintiffs-Appellees at 3, Arista Records LLC v. Doe 3, 2009 WL 414060 (N.D.N.Y 2009).

115. Memorandum of Law in Support of Ex Parte Application for Leave to Take Immediate Discovery at 3, Arista Records LLC v. Does 1-22, 2008 WL 5368436 (N.D.N.Y. 2008) (No. 1:08-cv-00765-NPM RFT). The Family Education Rights and Privacy Act 20 U.S.C. § 1232g (1974) requires that schools must obtain the permission of the student before releasing "educational records" to an inquiring party. The act broadly defines student records as, "those records, files, documents, and other materials which . . . . contain information directly related to a student." *Id.* at § 1232g (4)(A)(4). Whether or not providing information of the student's identity to the inquiring party would violate this act is beyond the scope of this Comment but warrants further consideration.

116. Memorandum of Law in Support of Motion to Quash, Arista Records LLC v. Does 1-16, 2008 WL 5368436 (N.D.N.Y. 2008) (No. 1:08-cv-00765-NPM RFT).

117. *Id*.

118. *Id*.

privilege afforded by the First Amendment.[119] Building off the "well established" understanding that "the First Amendment protects the right to speak anonymously," the defendants next merge the terms "speech" and "communicate," and argue that "First Amendment rights are fully applicable to communications over the internet."[120] This allows their deduction that any *communications* over the Internet, including copyright infringement, are protected under the "essential constitutional privilege" of the First Amendment.[121]

The District Court agreed that the "First Amendment protection extends to *expression* on the Internet."[122] The court admitted that, while the First Amendment affords a degree of protection to "anonymous expressions by an Internet user," the "expectation of privacy is limited" because "*expression* qualifies as speech only to a finite degree."[123] The court reasoned that although the First Amendment is not a "safe haven for copyright infringement,"[124] it does afford an "exceedingly small" privacy interest.[125] This "minimally protected constitutional right" of the alleged infringer, the court noted, must be weighed against the interest of a copyright owner. Refusing the discovery order, the court observed, would have an irreparable effect on the Plaintiffs' interests: "Without [the ISP] making available its list of allocated IP addresses to individual students so that a culprit of copyright infringement may be traced, Plaintiffs would be forever stymied in their efforts to protect their property rights and to bring an action against those alleged wrongdoers."[126] The court then concluded that the defendants' right to anonymity must "yield" to the Plaintiffs' interest in the information necessary to pursue their claims, and denied Defendants' motion to quash the subpoena.[127]

---

119. *Id.*

120. *Id.*

121. *Id*.

122. Arista Records v. Does 1-16, 2009 WL 414060, at *3 (N.D.N.Y. 2009) (emphasis added).

123. *Id.* (emphasis added).

124. *Id*. (citing *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 260 (D.D.C., 2003)).

125. *Id*.

126. *Id*. at *6.

127. *Id*.

The Defendants appealed the District Court's denial to the Court of Appeals for the Second Circuit, where the decision awaits review.[128] The Defendants raised the same three primary defenses as they did before the District Court.[129] In support of their First Amendment argument, Defendants claimed, "downloading, distributing, or making music available constitutes protected First Amendment speech."[130] Defendants claimed that this presumption affords them a "qualified privilege" to "communicate anonymously" that must be weighed against the Plaintiffs' interest in enforcing their copyrights.[131]

Plaintiffs respond by denying that the First Amendment affords any privilege to the type of activity at issue in the case.[132] Although there was a split in authority, Plaintiffs urged the Appellate Court to adopt the following rationale: "[m]any courts [who have] held that the act of infringing copyrights by downloading and distributing copyrighted works over a P2P network is not speech warranting First Amendment protection."[133] Without First Amendment protection, Plaintiffs argue the Defendants should have no expectation to any legally guaranteed anonymity.[134]

Three important issues were raised in this case. First, whether the Second Circuit agrees with the Plaintiffs or Defendants, Internet users assume a general, but prevalent, *presumption* of online anonymity that requires judicial action to overcome.[135] This is in large part due to the use of IP addresses and the lack of any corresponding directory or established

---

128. Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2nd Cir. Apr. 22, 2009).

129. *See supra* text accompanying notes 116-18.

130. Brief of Defendant-Appellant at 20, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2nd Cir. Apr. 22, 2009) (citing Sony Music Ent. v. Does 1-40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004); Fonovisa, Inc. v. Does 1-9, 2008 U.S. Dist. LEXIS 27170 at *29 (W.D.Pa. Apr. 3, 2008)).

131. *Id*.

132. Brief of Plaintiffs-Appellees at 16, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2nd Cir. Apr. 22, 2009).

133. *Id*. at 17.

134. *Id*. at 18.

135. This assertion is clearly supported by the current procedural requirements in any John Doe action: the identity of the anonymous user may only be demanded and discovered through subpoenas. *See* HART, *supra* note 7, at 33-42 (discussing how courts have treated John Doe cases and the requirements to subpoena necessary information to continue the suit).

procedures to discover the true identity.[136] Second, the ISP is presumed to be the protector of its end-user's identity and to have an obligation to refuse any inquiries unless accompanied by a court ordered subpoena.[137] Finally, the degree to which a person is afforded anonymity is directly correlative with their online activities at dispute in the controversy.[138]

A. Presumption of Anonymity

First, the presumption must be reassessed and defined in terms that shift the burden to ensure anonymity from the ISPs to the end-users. The presumption of anonymity finds its roots in the First Amendment, with the relevant part requiring, "Congress shall make no law . . . abridging the freedom of speech . . . ."[139] While a right to anonymity has been, or has attempted to be, extended to various types of activities, it originally applied squarely to "speech."[140] One such form of speech protected by the First Amendment is anonymous speech, which has recently been extended to anonymous speech on the Internet.[141] The migration and engrafting of anonymity to Internet communications has largely been the result of two

---

136. *See supra* notes 86-87 and accompanying text.

137. ISPs have a unique role as the gatekeeper to the anonymous users identities because it alone assigns each subscriber an IP addresses, and retains the logs and information that show which subscriber was assigned a particular address at a given time. While copyright owners have utilized services to discover the IP addresses of users who have unlawfully shared copyrighted files, they are unable to continue litigating their claim until the numerical IP address is translated into identifying information. *See* Press Release, RIAA, New Wave of Record Industry Lawsuits Brought Against 532 Illegal File Sharers (Jan. 21, 2004), *available* at http://www.riaa.com/newsitem.php?id=7A2318DB-1A51-7911-AB93-54D8337A9B90 (last visited Dec. 23, 2009).

138. For example, the First Amendment protects anonymity if the case "involve[es] core First Amendment expression." *In re* Verizon Internet Servs., Inc., Subpoena Enforcement Matter, Recording Indus. Ass'n of America v. Verizon Internet Servs., Civil Action No. 03-MS-0040, 257 F. Supp. 2d 244, 259 (D.D.C. 2003).

139. U.S. CONST. amend. I. *See* McIntyre v. Ohio Election Comm'n, 514 U.S. 334 (1995) (holding that Ohio's statutory prohibition against distributing anonymous campaign literature violated the First Amendment).

140. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) (noting that "The right to speak anonymously was of fundamental importance to the establishment of our Constitution").

141. Reno v. ACLU, 521 U.S. 844, 870 (1995) (reviewing First Amendment Supreme Court jurisprudence and noting that "our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]."); *accord*, Sinclair v. TubeSockTedD, 596 F. Supp. 2d 128, 131 (D.D.C. 2009) ("Such rights to speak anonymously apply . . . to speech on the Internet.")

factors. First, the Internet is architecturally supported by systems that, as a matter of technical design and efficiency, allow free access and use of the Internet, across a variety of mediums.[142] Moreover, because it is common practice for ISPs to randomly assign IP addresses to the user with each distinct connection (this type of IP address is called a *dynamic* address) and only *may* store identifying information within their system logs, an individual may communicate under different IP addresses several times a day.[143] Accordingly, matching the user with their online activity is usually only possible with the help of the ISP, help that must usually be compelled through judicial procedures.[144] Even assigning fixed IP addresses (*static* addresses) limits knowledge of the real identity of the end-user to the ISP,[145] since there is currently no public register or directory that matches IP addresses to users.[146] Second, the Internet provides users with "the

---

142. NICOLL, *supra* note 19, at 102-05. Almost fourteen years ago the Supreme Court observed how the Internet "provides relatively unlimited, low-cost capacity for communication of all kinds." The Court further noted:

> This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. 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. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.

Reno, 521 U.S. at 870.

143. NICOLL, *supra* note 19, at 102.

144. In *Call of the Wild*, Time Warner and supporting Amici did not "dispute that the plaintiffs have no other sources for the information they seek." No. 10-455 BAH, at 25. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 205 (2004) (noting "an ISP often holds the key to one's ability to communicate anonymously on the Internet).

145. Static addresses provide a significant advantage over dynamic addresses for purposes of discovering the identity of an individual, but, under the most widely-used IPv4 framework, static addresses are uncommon and inefficient for most consumer usage. *See* K. Hubbard et al., *Internet Registry IP Allocation Guidelines* 6 (Network Working Group, Internet Engineering Steering Group, Request For Comments No. 2050, Nov. 1996), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc2050.txt.pdf.

146. The plausibility of an Internet "white pages" or "yellow pages" is currently untenable because such a registry would require static addressing. The majority of the Internet currently relies on IPv4 for address assignment. This protocol allocates 32-bit IP address, which limits the number of possible devices attached to the Internet to 232. This makes it impossible to universally assign dynamic addresses, and, accordingly, ISPs rely heavily on dynamically assigning addresses to accommodate subscribers. However, with the number of devices accessing the Internet increasing daily, the number of IP addresses will eventually be exhausted under IPv4, so individuals and network administrators will soon be

greatest choice in what identity pointers . . . to reveal."[147] Functionally, this allows individuals who are at first identifiable only by their numerical IP address to choose what additional information to disclose.[148]

B. The Unique Position of ISP as Gateway to the End-Users

The second observation, and one closely related to the first, is that ISPs are placed *de facto* in a unique position as the guardian and caretaker of its subscribers' identities.[149] In most instances, any attempt to force disclosure of an identity will eventually lead the inquiring party to the ISP, even after third-party content providers submit to disclosure demands.[150] Moreover, because ISPs provide access to the Internet, physical storage of data, and systems used by subscribers and others on the Internet, they may be liable for any abuse or illegal use of the services provided.[151] However, even when the ISP plays a completely passive role by only providing Internet access to an end-user, the ISP has the burden of deciding when, to whom, and under what circumstances the end-user's identity may be revealed.[152]

C. Anonymity: A Matter of Degree or Categorical Assumption?

Finally, courts seem to follow the principle that anonymity is a matter of degree, measured by the activity to which it seeks to extend.[153] Even within the context of "speech," the First Amendment provides only limited anonymity.[154] For example, where the 'speech' is copyright infringement,

---

forced to adopt IPv6, which utilizes 128-bit addresses and provides 2128 possible devises to connect to the Internet simultaneously. Although the Internet is far from comprehensive implementation of IPv6, the move towards IPv6 is imminent. (For example, a group of large Internet companies have agreed to begin enabling IPv6 on "World IPv6 Day"—June 8, 2011. http://isoc.org/wp/worldipv6day/). Since static addressing would be more plausible under IPv6, the viability of an address/subscriber registry would be possible.

147. NICOLL, supra note 19, at 100. *See* discussion *supra* Part I.A.

148. NICOLL, supra note 19, at 100. *See also supra* note 26.

149. *See supra* note 144 and accompanying text.

150. *Id.*

151. The DMCA was enacted largely to address these issues. *See supra* Part II.C.

152. *See* Raynolds, *supra* note 72, at 373 (noting "the ISP remains a central, significant, and highly involved third-party because it is responsible for transferring requests and information to and from the RIAA and the user").

153. Arista Records LLC, v. Does 1-16, 2009 WL 414060, at *3 (N.D.N.Y. 2009) (citing Music Ent. v. Does 1-40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004)).

154. *Id.*

the privacy interests are "exceedingly small."[155] Within the scope of Internet activity, the U.S. Supreme Court has held that "First Amendment rights are fully applicable to communications over the [I]nternet."[156] But not all "communication" is awarded First Amendment shielding. Determining which activities deserve First Amendment protection requires the balancing of various factors.[157]

This inquiry is of significant importance in the case at hand. Both the Plaintiffs and Defendants acknowledge that certain activities are protected by First Amendment anonymity, but they disagree sharply on how this is to be applied.[158] Defendants assert a broad application of the term "speech" to include: "downloading, distributing, or making music available."[159] They contend that anything within the category of "speech" must be weighed against a party's "substantial and particularized" interest.[160] Plaintiffs do not disagree with the claim that First Amendment protected speech provides a qualified privilege, but they categorically disagree that any Internet "communication" is presumptively a form of "speech."[161]

There are many more issues raised in this case than those listed here, but the three issues discussed above are especially significant in most legal disputes involving the identity of an Internet user. A right to anonymity has become so broadly assumed that it is almost treated as a "fundamental right" requiring a substantial showing to overcome.[162] This places a

---

155. Arista Records LLC v. John Does 1-19, 551 F. Supp. 2d 1, 8 (S.D.N.Y. 2008).

156. *See* Brief of Defendant-Appellant at 20, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2nd Cir. Apr. 22, 2009).

157. *See Does 1-16*, 2009 WL 414060, at *4.

158. The agreement and disagreement between the parties exhibits an important observation: that "[t]he law does not determine what privacy is, but only what situations of privacy will be afforded legal protection." Hymen Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 36 (1967) *quoted in* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 39 (2d ed. 2009) (noting that "[p]rivacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be) legally protected").

159. Brief of Defendant-Appellant at 20, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2nd Cir. Apr. 22, 2009) (citing Sony Music Ent. v. Does 1-40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004); Fonovisa, Inc. v. Does 1-9, 2008 U.S. Dist. LEXIS 27170, at *29 (W.D. Pa. April 3, 2008)).

160. Brief of Defendant-Appellant at 20, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2d Cir. Apr. 22, 2009)

161. Brief of Plaintiffs-Appellees at 17, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2d Cir. Apr. 22, 2009).

162. *See* Brief of Defendant-Appellant at 21, Arista Records LLC, v. Doe 3, 2009 WL 414060 (N.D.N.Y. 2009), *appeal docketed*, No. 09-0905-cv (2d Cir. Apr. 22, 2009).

tremendous burden on ISPs to act as a guardian and protector of their subscribers' identities. Without becoming actively involved in any illegal activity, this assumed role entangles ISPs in any legal action against a subscriber.

IV. RETHINKING ISP ROLE AS GUARDIAN AND PROTECTOR

Since its genesis in 1998, the DMCA has played a tremendous role in the development of the Internet and has been hailed as "the law that saved the web."[163] Despite several shortcomings, the DMCA has proven successful, and arguably crucial, in accommodating many cultural and business Internet trends over the past decade.[164] The DMCA will continue to be a vital piece of legislation supporting the developing Internet; however, several key issues must be resolved. First, the scope and limits of First Amendment protection pertaining to Internet communications must be clearly defined. Second, as the Internet develops, the Internet culture must be held to a higher standard of responsibility.[165] In a sense, the "age of innocence" has passed, and subscribers and end-users must be responsible for their activities and the protection of their identity.[166] Third, the DMCA should be amended, or reinterpreted, to provide legal procedures to acquire the identity of anonymous users from ISPs. Finally, in the alternative to the third issue, courts should interpret the DMCA to accommodate contemporary trends by reading section 512(a) as only limiting ISP's secondary liability if the ISP complies with a copyright owners request for an infringers' identifying information.

---

163. David Karvets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later.

164. *Id*.

165. Internet content providers are beginning to notice this need and react accordingly. *See* Julie Zhuo, *Where Anonymity Breeds Contempt*, N.Y. TIMES, Nov. 30, 2010, at 31 (noting that "until the age of the Internet, anonymity was a rare thing. When someone spoke in public, his audience would naturally be able to see who was talking" and noting a negative consequence to Internet anonymity as "online disinhibition effect": "Psychological research has proven again and again that anonymity increases unethical behavior. Road rage bubbles up in the relative anonymity of one's car. *And in the online world, which can offer total anonymity, the effect is even more pronounced*. People—even ordinary, good people—often change their behavior in radical ways." *Id.* (emphasis added))

166. Zhuo, *supra* note 165.

A. Limits to First Amendment Protection: Distinguishing Source and Content

First Amendment protection, while extending to "expression on the Internet,"[167] does not extend to copyright infringement[168] and affords such communications only an "exceedingly small" privacy interest.[169] What "exceedingly small" privacy interest the First Amendment *does* afford is unsettled.[170] In *In re Verizon* the court measured "the degree of protection" by the type of conduct in question.[171] Since copyright infringement was alleged, the protection afforded was minimal.[172] This measurement of protection, the court in *In re Verizon* held, is determined in the pleadings: "In order to obtain a subpoena, the copyright owner must, in effect, plead a prima facie case of copyright infringement."[173] Many fear that permitting a plaintiff to unveil the identity of an individual after meeting such minimal requirements—alleging wrongdoing—could have a "serious chilling effect on anonymous speech."[174] However, this requirement is also a sensible and logical approach to John Doe litigation.

The First Amendment provides various degrees of protection to both the individual engaging in the communication and the actual content therein.[175]

---

167. Arista Records v. Does 1-16, 2009 WL 414060, at *5 (N.D.N.Y. 2009).

168. *Id. See In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 260 (D.D.C., 2003); *see also* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000) (citing Harper & Row Publishers, Inc. v. Nation Enters, 471 U.S. 539, 555-560 (1985)).

169. Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) ("First Amendment privacy interests are exceedingly small where the 'speech' is the alleged infringement of copyrights.").

170. *Compare* Sony Music Ent. v. Does 1-40, 326 F. Supp. 2d 556, 564 (S.D.N.Y. 2004) (finding defendant's alleged conduct of P2P file copying qualified as an exercise of speech, but only to a degree), *with* A&M Records v. Napster, Inc., 239 F.3d 1004, 1028 (9th Cir. 2001) (holding that the First Amendment does not protect use of a P2P file-sharing network that constitutes copyright infringement).

171. *In re Verizon*, 257 F. Supp. 2d at 260.

172. *Id.*

173. *Id.* at 263.

174. Brief of Defendant-Appellant at 21, Arista Records LLC v. Doe 3, No. 09-0905-cv (2d Cir. Mar. 26, 2009).

175. The distinction between these two is critical in cases involving anonymity. There exists a "recognized right to speak and write anonymously and to participate anonymously in group activities." *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084 (1961) (discussing the debate over the constitutional "freedom of anonymity"). However, not all content of speech and communication is constitutionally protected. *See, e.g.*, FCC v. Pacifica Found., 438 U.S. 726 (1978) (noting that the

In Internet copyright infringement cases the dual First Amendment protections can be seen as protecting what a person *does* online (conduct and content), and who an individual *is* while online (source).[176] This distinction between conduct or content and source is important in determining what degree of protection the First Amendment affords.[177] The conduct of an individual leads to matters of the *source* of that conduct and relates directly to issues of identity. Any content produced by a person's online conduct is an issue of subject matter, and is loosely or indirectly related to the identity of the individual. Courts already consider the content in question when evaluating and determining the degree of First Amendment protection afforded to the conduct and identity of the individual,[178] but both categories deserve special individual attention.

First Amendment protection extends to a wide range of content on the Internet. In *Reno v. ACLU*, the U.S. Supreme Court unanimously held that speech on the Internet is entitled to the full First Amendment protection extended to newspapers and other print media.[179] In *Reno*, the Court considered the constitutionality of the Communications Decency Act, which prohibited "the knowing transmission of obscene or indecent messages to any recipient under 18 years of age."[180] The term "transmission" refers to emails, file-sharing, and other "indecent communications."[181] The Court found the Act unconstitutional as a violation of the First Amendment, concluding that "[t]he interest in encouraging freedom of expression in a democratic society outweighs any

---

"government must remain neutral in the marketplace of ideas," but that "the constitutional protection accorded to a communication containing such patently offensive sexual and excretory language need not be the same in every context"). *Id*. at 737-47.

176. *See*, *e.g.*, Osborne v. Ohio, 495 U.S. 103 (1990) (holding that a state's compelling interest in prohibiting child pornography justifies laws banning mere possession of such materials). But in civil cases, courts are hesitant to force the disclosure of anonymous users' identities and require that the seeking plaintiff follow strict procedural requirements to convince the courts that a breach of the First Amendment privacy right is necessary. *See* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999).

177. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) (comparing Internet users communicating in "chat rooms" to the "pamphleteer" in Talley v. California, 362 U.S. 60 (1960), thus extending the high level of First Amendment protection to communications over the Internet).

178. *See supra* note 139.

179. *See generally Reno*, 521 U.S. at 844-45.

180. *Id*. at 859.

181. *Id*. at 867, 894.

theoretical but unproven benefit of censorship."[182] In the decade since *Reno* was decided, the scope of First Amendment protection in the Internet, and what qualifies as a constitutionally protected "communication," has been widely debated and refined.[183]

Freedom of speech protection has been limited or withheld from three primary types of content communicated over the Internet: obscenity (specifically child pornography),[184] defamation and libel,[185] and copyright infringement.[186] After the decision in *Reno* was handed down, Congress enacted a series of legislation attempting to prohibit the sharing of child pornography over the Internet.[187] Each enactment has been adjudicated and refined to comport to the First Amendment, but the general rule now accepted is that it is unlawful to "knowingly possess" child pornography.[188] Although transmitting and sharing contraband images and videos are forms of "communication," their illicit *content* is of a subject matter that is permissibly regulated.

Similarly, libelous and defamatory statements have limited First Amendment protection on the Internet. The Internet proffers seemingly unrestricted communication to an international audience. As one scholar notes:

---

182. *Id*. at 885.

183. *See* Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743 (2003) (noting "the effect of advancing technologies on constitutional interpretation" addressed in *Reno* and subsequent courts urging individuals to "understand that responsibility as an unavoidable cost of enjoying freedom of speech." *Id.* at 778 n.155, 778).

184. *See* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996), *cert denied*, 519 U.S. 820 (1996) (finding couple guilty of knowingly transporting obscene files in interstate commerce under a federal obscenity statute because of a computer bulletin board service).

185. *See* Scheff v. Bock, No. 03022837 (Fla. Cir. Ct. Spt. 19, 2006) (ordering blogger to pay judgment of $11.35 million to Sue Scheff, the head of a child services referral company for calling her a "fraud" and a "con artist" on a blog).

186. *See* N.Y. Times Co. v. Tasini, 533 U.S. 483 (2001) (finding publishers that allowed third parties to republish online articles by freelance writers originally published in print without obtaining the writers' permission violated the writers' copy rights).

187. *See e.g.*, 18 U.S.C. § 2252A; Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003, Pub. L. No. 108-21, 117 Stat. 650 (2003); "Children's Internet Protection Act," Pub. L. No. 106-554 47 (47 U.S.C. § 254(h)(6) (2002) and 20 U.S.C. § 9134(f)(1) (2003)).

188. *See, e.g.*, United States v. Stulock, 308 F.3d 922 (8th Cir. 2002) (upholding defendants conviction for possession of child pornography after investigators found three images of child pornography in the cache on defendant's computer).

> The "old" mass media—newspapers, magazines, books, and broadcasters—place a gatekeeper between the speaker and her audience. The Internet removed that gatekeeper, allowing more speakers than ever before to reach a mass audience. The resulting "democratization of discourse" made it harder for those in power to control the interpretation of public events and exposed them to criticism from new quarters.[189]

Of the variety of forums on the Internet available to the "mass audience," blogs and online message boards are the subject of tremendous controversy, and often give rise to litigation for libelous remarks.[190] As "those who are the subjects of unflattering anonymous speech" seek to redress their grievances, they face the same difficulties in identifying the attacker and often bring suits against "John Doe" defendants.[191] Message boards and blogs are deemed public forums, and the anonymity of those who communicate in these forums is rigorously protected as an important privacy right.[192] Accordingly, discovering the identity of an individual who made allegedly defamatory remarks will prove to be difficult for the plaintiff.[193]

In many situations, individuals and their communications are protected by the third-party that provided the means for communication. Certain services, such as online newspapers and weblog publishers, will very often resist inquiries into the identity of bloggers and commentors, and will faithfully resist subpoenas.[194] In situations where communications are not made under the protective umbrella of a third-party, however, the expectation for privacy tends to revert to the ISP, which may have had very

---

189. Lyrissa B. Lidsky, *Anonymity in Cyberspace: What Can We Learn From John Doe?*, 50 B.C. L. REV. 1373, 1375 (2009) (discussing the issue of anonymity in libel lawsuits against Internet defendants).

190. *See* Laura Parker, *Courts Are Asked to Crack Down on Bloggers, Websites*, USA Today (Oct. 3, 2006), *available at* http://www.usatoday.com/tech/news/2006-10-02-bloggers-courts_x.htm.

191. HART, *supra* note 7, at 33-35.

192. *See* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (noting a "legitimate and valuable right to participate in online forums anonymously or pseudonymously" that must be weighed against "the need to provide injured parties with an forum in which they may seek redress for grievances").

193. *See, e.g.*, Doe v. 2TheMart.com, 140 F. Supp. 2d 1088 (W.D. Wash. 2001). *See also*, Jon Hart & Michael Rothberg, *Anonymous Internet Postings Pit Free Speech Against Accountability*, WSJ.COM (Mar. 8, 2002), http://online.wsj.com/public/resources/documents/SB1015251972510360720.htm.

194. *See, e.g.*, Enterline v. Pocono Med. Ctr., 751 F. Supp. 2d 782 (M.D. Pa. 2008).

little involvement in the communication message, or the methods used to communicate.

B. Place the Burden on the End-User

The Internet has developed to the point where ISPs should no longer be expected to shield the identity of their subscribers from inquiring litigants. As the on-line culture matures and evolves, the individuals who connect to it naturally become more tech-savvy, use more on-line services, and become more informed of their rights and responsibilities. The average *reasonable* user should, accordingly, be presumed to understand the consequences of his actions, and able to determine the means to protect their interests.[195] In terms of the on-line piracy that this Comment has addressed, the reasonable user likely understands that sharing copyrighted files is generally unlawful, and, at *least*, mindful of the danger of litigation or prosecution if caught pirating materials.[196] In a sense, the age of innocence and naiveté has passed, and the individual should now be held to an enlightened position, responsible for his actions and accountable for his conduct, both online and offline.[197]

As part of this new era, the expectation of privacy and anonymity on the Internet must be reexamined. Criminal law, particularly the area of law dealing with privacy expectations under the Fourth Amendment, offers an excellent resource for analysis.[198] In *Katz v. United States*, the Supreme

---

195. Close to eighty percent of the United States population currently have Internet access, a remarkable growth from the limited 0.8% in 1990. *Internet Users as a Percentage of Population*, GOOGLE, http://www.google.com/publicdata?ds=wb-wdi&met_y=it_net_user (select "World" or individual country under "Public Data" column on left) (last visited June 20, 2011).

196. For example, following the recent introduction of Sweden's attempt to pass anti-piracy legislation known as IPRED, one technology group noted that the country saw a thirty percent drop in network traffic. They noted that "[m]any attributed this fall to Internet users become [sic] scared that they would be caught downloading and sharing copyright material." *Illicit File-Sharing and Streaming of TV Shows Increases*, TORRENTFREAK (Feb. 17, 2010), http://torrentfreak.com/illicit-file-sharing-and-streaming-of-tv-shows-increases-100217/.

197. Sweden is an excellent example of a society where individuals *are* assuming responsibility for their own protection and taking active measures to hide their identity. As certain reports indicate, between six and seven percent of the Swedish population hide their identity while on the Internet. *Millions of File-Sharers Hide Their Identities Online*, TORRENTFREAK (Nov. 3, 2009), http://torrentfreak.com/millions-of-file-sharers-hide-their-identities-online-091103 (referencing a study undertaken by Måns Svensson, Ph.D. in Sociology of Law in Lund).

198. This Comment does not suggest that *all* Fourth Amendment implications are applicable here, only that the "reasonable expectation of privacy" test first proffered in *Katz*

Court established the "legitimate expectation of privacy" test.[199] Considering what privacy rights an individual has, even when allegedly conducting illegal activities, the Court applied a two-part test: first, did the individual possess a *subjective* expectation of privacy, and second, was that expectation *objectively* "one that society is prepared to recognize as 'reasonable.'"[200] Although this inquiry is intended to define whether an individual is afforded privacy rights under the Fourth Amendment, the rationale and logic behind this analysis is profoundly applicable to expectations of anonymity privacy on the Internet.[201]

The first part of the *Katz* test considers whether an individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy."[202] Broadening this inquiry and applying it to Internet users as a whole presents an interesting question: what degree of privacy *does* the average reasonable user expect? But this cannot be easily or even generally answered. Each activity or transaction on the Internet carries its own expectations.[203] For example, a bidder on eBay may expect that his limited online profile will be revealed to other bidders, while his true identity along with financial information will be revealed to the seller if he succeeds in outbidding

---

and *Smith* translates well in civil law contexts. *See, e.g.*, CAL. CIV. CODE § 1708.8(b) (West) (constructing civil liability for invasion of privacy: "A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a *reasonable expectation of privacy*") (emphasis added).

199. 389 U.S. 347 (1967); *see also* Smith v. Maryland, 442 U.S. 735, 738 (1979) (naming and applying the "reasonable expectation of privacy" test to pen registers).

200. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

201. The Internet protocols for many online forms of communication still resemble, and arguably rely on, the communication technology at issue in both *Smith* (decided in 1979) and *Katz* (1979). *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (concluding that "the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in Smith."); *In re* Application for an Order Authorizing use of A Pen Register And Trap On (XXX) Internet Service Account/User Name, (xxxxxxxx@xxx.com), 396 F. Supp. 2d 45 (D.Mass. 2005) (considering the use of pen registers and trap and trace devices to monitor Internet account activities). *See also* Doe v. Prosecutor, Marion Cnty., Ind., 566 F. Supp. 2d 862, 881 (S.D. Ind. 2008) (applying other principles of Fourth Amendment jurisprudence to searches of computers and noting "If monitoring does not invade genuine private content, then there may be no search subject to the Fourth Amendment.").

202. *Id*. at 740.

203. *See supra* note 26 and accompanying text.

others.[204] However, this expectation of privacy is related more to the individual's financial interests than the legality of his transactions. Similarly, individuals may assume that their Google searches, blog posts, or other online activities are awarded a degree of privacy that prohibits unwarranted inquiries.[205] In contrast, in a post-Napster takedown era, it would be hard to find anyone who is unaware that involvement in unlawful file-sharing poses potential legal actions and penalties.[206] In theory, a multi-tasking Internet user may browse blogs, the web shop on eBay, and be running file-sharing software downloading unauthorized material simultaneously, with his expectation of privacy varying with each activity.[207] Therefore, individuals' expectation of privacy may generally be assumed as directly relating to the type of activity or content the individual views, shares, or downloads on the Internet.

The second part of the *Katz* test asks, "whether the individual's subjective expectation of privacy is one that society is prepared to recognize as 'reasonable.'"[208] This inquiry produces a broad and interesting range of answers and opinions. As a preliminary matter, it is important to note that the debate over anonymity is largely focused on *which* activities deserve anonymity.[209] This Comment, however, is focused on the procedures to discovery identity, and necessarily assumes that there are instances where the right to anonymity is outweighed by the right or interest served in litigating a dispute.[210] Accordingly, the question turns on *who*

---

204. *Bidding Overview*, EBAY, http://pages.ebay.com/help/buy/bidding-overview.html (last visited Apr. 22, 2011).

205. The legitimacy of this expectation is currently a hot topic as the recent introduction of 'Google Buzz' has prompted public concern and a class action lawsuit. *See* Nicholas Carlson, *WARNING: Google Buzz Has a Huge Privacy Flaw*, BUSINESS INSIDER (Feb. 10, 2010), *available at* http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2.

206. *See supra* notes 197-98.

207. *See supra* note 26 and accompanying text.

208. *Smith*, 442 U.S. at 740 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

209. *See supra* note 158.

210. Courts often apply a balancing test in these cases. *See, e.g.*, John Doe v. 2theMart.com, 140 F. Supp. 2d 1088 (W.D. Wash. 2001). In adopting a standard for "evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation," the court weighed whether:

> (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to

protects the user's identity, or *how* anonymity is afforded. To explain this distinction, it is necessary to consider the structure of the Internet and its various components.

As discussed above, an individual accessing the Internet from his home, work, or school has some form of contractual relationship with the ISP.[211] Once connected to the Internet, most websites the individual visits[212] will also stipulate some form of contractual terms of service agreement.[213] Email

---

> that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.

Id. at 1095.

211. For example, Comcast, one of the largest Internet providers in the United States, explicitly addresses in all capital letters:

> YOU AGREE THAT YOU SHALL BE RESPONSIBLE FOR AND SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS COMCAST AND ITS EMPLOYEES, AFFILIATES, SUPPLIERS, AGENTS AND CONTRACTORS AND SHALL REIMBURSE US FOR ANY DAMAGES, LOSSES OR EXPENSES (INCLUDING WITHOUT LIMITATION, REASONABLE ATTORNEYS' FEES AND COSTS) INCURRED BY US IN CONNECTION WITH ANY CLAIMS, SUITS, JUDGMENTS, AND CAUSES OF ACTION ARISING OUT OF (a) YOUR USE OF THE SERVICE OR COMCAST EQUIPMENT; (b) VIOLATION OR INFRINGEMENT OF CONTRACTUAL RIGHTS, PRIVACY, CONFIDENTIALITY, COPYRIGHT, PATENT, TRADEMARK, TRADE SECRET, OR OTHER INTELLECTUAL PROPERTY AND PROPRIETARY RIGHTS ARISING FROM YOUR USE OF THE SERVICE OR ANY UNAUTHORIZED APPARATUS OR SYSTEM.

Comcast Agreement for Residential Services, COMCAST, *available at* http://www.comcast.com/Corporate/Customers/Policies/SubscriberAgreement.html (last visited Apr. 10, 2011).

212. It is important to remember that a person may still rely on pseudonyms with any online activity, so the information governed by EUAs is somewhat limited in how effective they are. The information retained, when not linked directly to financial information, may still not contain any positive identifying information.

213. For example, Facebook declares in its terms of service that:

> By using or accessing Facebook, you agree to this Statement. . . . (1) For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it. (2) When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in

services almost universally regulate subscribers' use through the terms of service.[214] Some form of contractual relationship between the end-user and service provider governs almost every transaction, service, site visit, and activity that occurs on the Internet.[215] However, for those forms of communication, such as P2P file-sharing, where no intermediate content or service provider exists, no "terms of service" agreements govern the transactions between individuals.[216] And where no third-party is in a position to secure an individual's identity, the expectation of protection is presumed to, almost by default, shift to the ISP itself.[217] In these situations, where no controlling third party may be complained to or is in the position to control the end-user's activity, the ISP assumes a de facto position of regulating the user's activity (for example, by port blocking or terminating

---

> backup copies for a reasonable period of time (but will not be available to others).

Statement of Rights and Responsibilities, FACEBOOK.COM, http://www.facebook.com/terms.php (last visited Apr. 10, 2011)

214. For example, Gmail's "Privacy Policy" states that Google:

> maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail.

Google Terms of Service, GOOGLE, http://www.tosback.org/diff.php?vid=1087 (last visited Apr. 23, 2011).

215. Some courts place tremendous weight on these contractual agreements, and interpret a subscriber's expectation of privacy based on the language in the terms of service. *See, e.g.*, Sony Music Entm't Inc. v. Does 1-40 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004).

216. Attempts to prosecute or sue individuals involved in P2P activities often have a difficult time determining who should be held liable. A noteworthy consequence of this structure can be seen in the controversial Swedish case against the Pirate Bay, a Swedish website that indexes BitTorrent files. Although the technology of indexing BitTorrent files does not involve the storage or communication of unlawful content, the Swedish court found the Pirate Bay administrators guilty of "assisting in making copyright content available." *The Pirate Bay Trial: The Official Verdict—Guilty*, TORRENTFREAK (Apr. 17, 2011), http://torrentfreak.com/the-pirate-bay-trial-the-verdict-090417. The legitimacy of claims against providers of indexers or trackers is beyond the scope of this Comment, but this is a subject that deserves significant thought and consideration.

217. The de facto subscriber/provider status will almost always be the last stop before reaching the individual user. This Comment acknowledges that "IP addresses aren't people" and that it merely identifies the subscriber's connection, which may be shared among many different people. Litigants may necessarily need to clear an additional hurdle by overcoming any defenses that the connection was *not* in the exclusive control or use of the owner.

service), or providing the user's information to requesting parties to allow further injunctive or judicial actions.[218]

Considering the second part of the *Katz* test under these observations, the question must necessarily be narrowed to: what is a reasonable expectation of privacy that an ISP should be expected to provide to its subscribers? The "expectation of privacy" in this instance may be very narrowly defined as: the disclosed association of a user's true identity with the IP address he or she was assigned at a given point in time. The DMCA responded to this question in part by rejecting any notion of anonymous privacy when the activities in question show a prima facie case of copyright infringement.[219] Therefore, there is no reasonable expectation of privacy where the activity in question is unlawful.[220] Procedurally, however, this conclusion misses a key issue: the ISP is still placed in the position as a form of content-regulator, despite its actual role as merely a passive gateway.[221]

Application of the *Katz* test in this context reveals two important observations: first, individuals are most likely aware that their expectation of privacy is directly related to their activities.[222] Accordingly, the degree of caution with which people access and share information is usually directly

---

218. These steps are often taken at the ISP's own initiative in an attempt to curb bandwidth overloads. *See* Fink v. Time Warner Cable, 2009 WL 2207920 (S.D.N.Y. 2009) (dismissing a nation-wide class action claim against Time Warner Cable for throttling BitTorrent use on procedural grounds). *But see* Declan McCullagh, *FCC Formally Rules Comcast's Throttling of BitTorrent was Illegal*, CNET NEWS (Aug. 1, 2008, 8:19 AM), http://news.cnet.com/8301-13578_3-10004508-38.html (reporting an order released by the FCC threatening to adjudicate disputes involving "discriminatory network management"). The availability of these restrictions, however, does not suggest ISPs should be *expected* to proactively implement them at the command of private parties, or submit to subpoena inquiries. *See* Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1235 (D.C. Cir. 2003) (holding that the DMCA does not permit the issuance of subpoenas when an ISP acts as a mere conduit for P2P file-sharing "because [ISPs] *do[] not control the content on its subscribers' computers*") (emphasis added).

219. *See* 17 U.S.C. § 512(h) (providing subpoena power to copyright owners upon "a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights").

220. *See Sony Music Entm't Inc.*, 326 F. Supp. 2d at 566 (S.D.N.Y. 2004) (finding "defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission").

221. *See supra* Part II.C.

222. *See supra* note 196.

related to the service or content provider with which they interact.[223] As an individual's finances, community reputation, and other protected interests become more vulnerable, the individual is more inclined to exercise greater care in choosing who they transact with, the content of their communications, and how they transmit the sensitive information.[224] Second, the law, in general, denies the privilege of anonymity when illegal conduct is in question.[225] Various laws provide procedural safeguards for service or content providers to limit their liability and provide procedural remedies for injured individuals to protect their interests.[226] These laws, in a sense, clear the way and create direct access to the party acting unlawfully, while limiting the collateral damage and unnecessary involvement to the passive agents whose services the individual has used in their unlawful actions.[227] For example, if a derogatory comment is made on an individual's Facebook "wall," or if an individual posts a defamatory "tweet" on Twitter, Facebook and Twitter will not be held liable.[228] Rather, if a legal action is brought against the commenter or "tweeter," Facebook and Twitter may choose to provide the user's information upon request, per the terms of

---

223. Julie Zhuo, a product design manager at Facebook, acknowledged in a recent New York Times article that "[c]ontent providers, social networking platforms and community sites must also do their part by rethinking the systems they have in place for user commentary as to discourage—or disallow—anonymity." Julie Zhuo, *Where Anonymity Breeds Contempt*, N.Y. TIMES, Nov. 30, 2010, at 31. Discussing the problem of Internet "trolls" (individuals who post "inflammatory, derogatory or provocative messages"), Zhuo noted that "most trolls wouldn't have the gall to say to another person's face half the things they anonymously post on the Internet." *Id.* Zhuo described her work on Facebook's commenting system, where "the approach is to try to replicate real-world social norms by emphasizing the human qualities of conversation," as creating a form of "social pressure" that works in reducing the problem of trolling. *Id.*

224. *Id.*

225. *See supra* Part II.C.

226. *See, e.g.*, 17 U.S.C. § 512(i) (limiting the liability of ISPs: "only if the service provider (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and (B) accommodates and does not interfere with standard technical measures").

227. *Id.*

228. Finkel v. Facebook, Inc., 2009 WL 3240365 (2009) (dismissing Facebook's motion to dismiss a defamation action against it for defamatory comments made in a "group page" on Facebook "because Facebook is immune from liability under the Communications Decency Act of 1996 as an interactive computer service").

service that govern the subscriber's relationship.[229] Therefore, it is reasonable to expect individuals to gauge the degree of privacy afforded in a particular forum by the content provider's terms of service, reputation for fighting or submitting to disclosure requests, and type of activities that the content provider permits.[230] Still, in the context of P2P applications where individuals connect directly with one another without third party mediation, what degree of expectation should an individual reasonably expect?

The logical conclusion first requires an acknowledgement that individuals understand their Internet activities are afforded only qualified privacy, the degree of which is determined in large part by the company providing the content or permitting the online activities.[231] These third parties are able to connect the *content* with the *source* of that content. Beyond the scope of third-party services, an individual is emancipated from moderators and 'terms of use,' but is also vulnerable.[232] Who he connects with, how he communicates, and what content is shared is, for the most part, determined by the individual.[233] However, if his conduct leads to legal action, his ISP may be forced to determine the degree of the subscriber's privacy it will fight to protect. But unlike other third-party service providers, ISPs have limited control or interaction with any *content* the subscriber may produce, and yet still hold the final key to the *source* of the content.

This Comment proposes that the party with the greatest control over the content communicated over the Internet be primarily responsible for protecting the source of that content. Accordingly, if the communications

---

229. *See, e.g.*, John Schwartz, *Twitter Fighting Pennsylvania Subpoena Seeking Names of 2 Tweeters*, N.Y. TIMES, May 20, 2010, at B4. Admittedly, Facebook or Twitter may only be able to provide the IP address associated with the account, but this still reflects the principle that this Comment argues should be adopted at the ISP level.

230. This is largely already the case. *See* Claire Cain Miller & Tanzina Vega, *Google Introduces a Social Tool, and Settles Charges Related to Another*, N.Y. TIMES, Mar. 31, 2011, at B3.

231. *See supra* notes 26, 212, 214 and accompanying text.

232. Many BitTorrent users understand the precarious position that this P2P protocol affords, and ban together behind "private trackers" (virtual communities where membership is by invite only). Ben Jones, *Trading BitTorrent Tracker Invites, Commodity or Curse?*, TORRENTFREAK (Jan. 15, 2008), http://torrentfreak.com/trading-bittorrent-tracker-invites-080115/. *But see* Enigmax, *Mass BitTorrent Lawsuits Now Target Private Trackers*, TORRENTFREAK (July 25, 2010), http://torrentfreak.com/mass-bittorrent-lawsuits-now-target-private-tracker-100725/ (reporting that even private trackers are targeted in mass BitTorrent lawsuits).

233. Ernesto, *Keep the Bad Guys Out*, TORRENTFREAK (Jan. 7, 2006), http://torrentfreak.com/keep-the-bad-guys-out.

involve direct P2P interaction, the individual should be primarily responsible for establishing their own rules, determining their own conduct, protecting their identity, and defending their privacy if an inquiry is brought.[234] While anonymity is a de facto status for many transactions in which the individual may reasonably assume full privacy, other communications provide very little or *no* expectation of privacy, and offer only illusory anonymity.[235] One such limited, self-regulating, form of communication is BitTorrent.[236]

Without narrowly confining this analysis to BitTorrent communications, a solution to the DMCA's shortcomings is simple: look to the *form* of communication to determine the propriety of a subpoena.[237] For example, if the conduct in question relates to a Facebook comment, the individual should expect the degree of privacy Facebook provides in their terms of service,[238] and subpoenas should be issued to Facebook if such terms do not protect the activity of the individual.[239] Additionally, if the conduct relates

---

234. *See supra* note 58. Because P2P file-sharing effectively places individuals in a position very similar to third-party service providers, this Comment argues that it is reasonable to assume they share a similar degree of liability.

235. *See supra* Part II.A–B.

236. *See supra* notes 65, 215, 217, 233.

237. To clarify: this relates *only* to revelation of the user's *identity*, not the *content* of their communications. *See supra* Part IV.A.

238. Privacy Guide, *supra* note 26.

239. The DMCA is currently applied in this manner in these types of cases, insofar as the content provider (i.e., Facebook) will not be held liable for most actions of their subscribers. *See supra*, notes 75-79 and accompanying text. Nevertheless, an inquiring may still only produce the IP address associated with the account, and the inquiring party will still need to convince the ISP to surrender the identity of the user. There is already a prevalent expectation that content providers establish clear and resolute privacy and protection standards. *See, e.g.*, Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011). This bill, introduced by John Kerry and John McCain, is designed "[t]o establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes." In the section addressing, entitled *Privacy By Design*, the relevant text reads:

> Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by—
>
> (1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on—
>
> (A) the reasonable expectations of such individuals regarding privacy; and
>
> (B) the relevant threats that need to be guarded against in meeting those expectations;

to a defamatory blog post with a blogging service that refuses to disclose a subscriber's identity unless required to do so by a court order, that individual has an expectation of privacy and subpoenas should not be issued until the conduct in question is deemed defamatory by a court and the individual may reasonably expect the blog provider to fight to protect her identity.[240] If, however, the conduct relates to unlawfully sharing copyrighted materials directly with other individuals, the infringer should be expected to defend himself against a copyright owner. Accordingly, a copyright owner should be able to acquire the individual's true identity by subpoena so long as the copyright owner presents a prima facie case for copyright infringement.[241] The individual may then show that there was no distribution, that the distribution was lawful, or even that the individual is a mistaken defendant—but, either way, it should be the *individual's* responsibility to defend his position.[242]

This solution will theoretically benefit ISPs in several ways. First, this would drastically reduce ISPs' need to involve themselves in litigation regarding the activities of their subscribers.[243] Most ISPs and content

---

Id. § 103. *But see Consumer Groups Welcome Bipartisan Privacy Effort, but Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy*, PR NEWSWIRE (Apr. 12, 2011), http://www.prnewswire.com/news-releases/consumer-groups-welcome-bipartisan-privacy-effort-but-warn-kerry-mccain-bill-insufficient-to-protect-consumers-online-privacy-119701399.html (highlighting the concerns of a privacy rights group, including a suggestion that: "Consumers must have the right to hold companies accountable for violating their privacy through a private right of action.").

240. *See supra* notes 190-94 and accompanying text.

241. The showing of a prima facie case is already the first prong in *Columbia*. *See supra* note 42, and accompanying text. Maintaining this requirement is important to prevent abusive litigation and to ensure that "people who have committed no wrong [are] able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

242. This Comment notes the controversial nature of this assertion in lieu of the extortion-like methods many copyright owners use to enforce their privileges, but suggests that if individuals were more informed of their rights and fought back in greater numbers, such litigation techniques would ultimately prove unprofitable for plaintiffs. For an excellent example of methods available to prospective defendants, see CHILLING EFFECTS, http://www.chillingeffects.org (last visited July 2, 2011); *How Not to Get Sued for File Sharing*, ELECTRONIC FRONTIER FOUNDATION (July, 2006), https://www.eff.org/wp/how-not-get-sued-file-sharing.

243. In *Call of the Wild* the ISP Time Warner contended that complying with a request seeking a large number of its subscribers would cause it to "'suffer significant harms' and 'incur significant costs' because compliance . . . would 'overwhelm' its capacity and

providers already defer to DMCA guidelines for taking down hosted infringing materials, and would arguably be equally deferent to more intelligible guidelines for revealing identities if such existed. Second, ISPs and society as a whole would benefit from neutral ISPs. The more an ISP resembles an obstacle in reaching end-users, the more likely that ISPs will be forced to take on other forms of censorship and policing.[244] But such a role should not be expected from companies that merely provide gateway access to the Internet. Finally, permitting easier discovery of P2P users' identities more accurately reflects the role of ISPs as a gateway, with minimal duties to defend or protect the *identity* of their subscribers.[245] Clarifying this role would reduce ISPs' fear that they are betraying their subscribers' trust while apprising end users that they are ultimately responsible for their online behavior.

Individuals may worry that such vulnerability nullifies any possibility of privacy or legitimate anonymity, but this fear is unfounded and incorrect. Rather, there are a variety of measures one may take to hide his unlawful activities, obscure his identity, and ensure his privacy. For example, the Pirate Bay, a popular file-sharing service provider, recently opened to the public a special VPN service that allows Internet access through a secured server that hides the originating IP address, and does not log the associated assigned IP address with the user. This effectively creates a third-party gateway that neutralizes the possibility to discover the end-user.[246] Other services, such as Tor or Privoxy, provide measures for individuals to communicate anonymously through a series of virtual tunnels.[247]

V. CONCLUSION

The DMCA has failed to adapt to changing technology. Burdening copyright owners with the preliminary requirement of discovering *who* has

---

'completely absorb the resources for many months.'" Call of the Wild Movie, LLC v. Does 1-1,062, CIV.A. 10-455 BAH, 2011 WL 996786, at *16, (D.D.C. Mar. 22, 2011).

244. *See* Matthew Lasar, *The Real Internet Censors: Unaccountable ISPs*, ARS TECHNICA (Feb. 10, 2011, 11:45 AM), http://arstechnica.com/web/news/2011/02/isps-the-off-duty-cops-of-the-world.ars.

245. *See supra* Part III.B.

246. Ernesto, *Pirate Bay's Ipredator VPN Opens to the Public*, TORRENTFREAK (Jan. 1, 2010), http://torrentfreak.com/pirate-bays-ipredator-vpn-opens-to-the-public-090120.

247. *Tor Project: Overview*, TOR, http://www.torproject.org/overview.html (last visited Apr. 9, 2011). *But see* Thomas Lowenthal, *Not Anonymous: Attack Reveals BitTorrent Users on Tor Network*, ARS TECHNICA (Apr. 12, 2011 10:57 AM), http://arstechnica.com/tech-policy/news/2011/04/not-anonymous-attack-reveals-bittorrent-users-on-tor-network.ars (noting that the popular anonymity tool still has vulnerabilities).

infringed upon their rights is an unnecessary encumbrance on protecting legitimate property interests. Because the DMCA stands as the primary body of legislation addressing the issues that arise with Internet piracy, it should be adorned with new provisions or interpretations that allow it to carry out its intended purpose. If the outmoded treatment of ISPs as agents to subscribers were discarded, the burdens of responsibility and accountability would return to individuals. While some courts have adopted a broad interpretation of the DMCA allowing for more liberal discovery methods, there is yet to be any affirmative policy recognition of the evolving Internet culture.[248]

Tools to limit an individual's vulnerability are becoming more accessible and more effective for the individual who seeks anonymous activity. As these technologies develop, the role of the average domestic ISP should be scaled back to what its primary function is: a gateway to the Internet. Courts and legislature should no longer consider or treat ISPs as *in loco parentis* of their subscribers' identity.

248. *See, e.g.*, Atlantic v. Does 1-25, No. 05-CV-9111 (D.N.Y. June 5, 2006) (denying motion to vacate ex parte discovery order); Motown v. Does 1-99, No. 05-CV-9112 (D.N.Y. Feb. 10, 2006) (dissolving stay of expedited discovery); Warner v. Does 1-149, No. 05-CV-8365 (D.N.Y. June 7, 2006) (denying motion to vacate ex parte discovery order and quash subpoena).