MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 38 | Issue 1 Article 6

2011

Bringing John Doe to Court: Procedural Issues in Unmasking Anonymous Internet Defendants

Robert G. Larson

Paul A. Godfread

BRINGING JOHN DOE TO COURT: PROCEDURAL ISSUES IN UNMASKING ANONYMOUS INTERNET DEFENDANTS

Robert G. Larson† and Paul A. Godfread††

I. INTRODUCTION

The Internet is ubiquitous. Over the past two decades, it has grown and evolved, overcome boundaries, and defied containment. The Internet can now be accessed not only through a designated computer terminal but on any number of devices: wireless laptop

† Robert Larson graduated from William Mitchell College of Law in 2010, is a registered patent attorney practicing in Minneapolis, Minnesota, and would like to thank his wife Heather and his family.

†† Paul Godfread graduated from William Mitchell College of Law in 2008, is an attorney practicing copyright and trademark law at Godfread Law Firm in Minneapolis, Minnesota, and would like to thank his wife Miranda and his family for their support. The author would also like to thank Professor Erlinder for working with him on the issue of the First Amendment and anonymous speech in 2008.

computers, cellular telephones, e-readers,[1] game consoles,[2] televisions,[3] cars,[4] and even refrigerators.[5] Unfortunately, while the Internet has undoubtedly made many aspects of our lives easier, it has also provided more opportunities to run afoul of the law, infringe intellectual property rights, and engage in tortious speech and activities.[6]

One of the predominant properties of the Internet is the general veil of anonymity. The Internet, in contrast with the real world, lacks many of the self-authenticating features that human society has come to rely on when identifying individuals.[7] In real life it is difficult to disguise one's identity, and the difficulty increases with familiarity because familiarity brings with it knowledge about a multitude of variables: one's appearance, one's tone of voice, one's physical movements, etc. But, on the Internet, familiarity is usually linked to a small handful of factors—often just a username and password combination.[8] If you have the correct

1. *See* Brad Stone, *In Price War, E-Readers Go Below $200*, N.Y. TIMES, June 22, 2010, at B1, *available at* http://www.nytimes.com/2010/06/22/technology/22reader.html?ref=technology.

2. *See Sony's PS3 Price Cut: Desperate, or Savvy Move?*, INT'L BUS. TIMES (Aug. 17, 2011), http://www.ibtimes.com/articles/199254/20110817/sony-ps3-price-cut-wii-xbox-360.htm.

3. *See* Forrest Hartman, *What Is an Internet-Enabled TV?*, ABOUT.COM, http://tv.about.com/od/frequentlyaskedquestions/f/InternetTVFAQ.htm (last visited Sept. 11, 2011).

4. *See* Brian Cooley, *Cadillac Rolls Out in-Car Internet Access*, CNET REVIEWS (Mar. 19, 2009, 4:00 AM), http://reviews.cnet.com/8301-13746_7-10199833-48.html.

5. *See, e.g.*, *LG Internet Refrigerator*, LG, http://us.lge.com/www/product/refrigerator_demo.html (last visited Sept. 11, 2011).

6. *See, e.g.*, Capitol Records, Inc. v. Thomas, 579 F. Supp. 2d 1210, 1212–13 (D. Minn. 2008) (involving an Internet user accused of illegal copyright infringement after sharing music files); Scheff v. Bock, No. 03-022837, 2007 WL 6930518, at ¶ 1 (Fla. Cir. Ct. July 25, 2007) (involving a lawsuit for defamation over written material published on the Internet).

7. LAWRENCE LESSIG, CODE: VERSION 2.0 45 (2006) ("The absence of relatively self-authenticating facts in cyberspace makes it extremely difficult to regulate behavior there.").

8. Although systems are being developed to expand the number of authenticating facts—for example, Google has begun to look for suspicious account activity, primarily by recording "the geographic region that [it] can best associate with the access"—many online services have not yet implemented advanced anti-fraud mechanisms. *See* Pavni Diwanji, *Detecting Suspicious Account Activity*, GOOGLE ONLINE SECURITY BLOG (Mar. 24, 2010, 9:15 AM), http://googleonlinesecurity.blogspot.com/2010/03/detecting-suspicious-account-activity.html. Furthermore, while sophisticated Online Service Providers (OSPs) may employ such measures, third parties—such as other users—frequently lack access to the wealth of data necessary for advanced identification processes.

username and password, the Internet doesn't doubt your identity. Simply having a different username and password typically leads the Internet to believe that you are a different person altogether.[9]

That anonymity makes many of the problems mentioned above much more difficult to resolve. Without a clearly identifiable defendant, a plaintiff has little chance of recovery, and while anonymous defendants are not a phenomenon unique to the Internet, the prevalence of the Internet in modern society has exacerbated this problem.[10] This article explores the mechanisms available to discover the identity of an otherwise anonymous Internet user, and discusses the complications—forum selection, service and notice, limited litigation tools available to anonymous defendants, opportunities for abuse, and burdens placed on disinterested third parties—inherent in litigating against an anonymous Internet defendant. In particular, the authors seek to call attention to the inequitable treatment of anonymous Internet defendants, as exemplified by the limitations placed on them during litigation, the ease with which procedural abuses can be inflicted upon them, the complicity of otherwise disinterested third parties in ignoring the privacy rights of anonymous Internet defendants, and the continued neglect—of both judicial and legislative bodies—in addressing such issues. To rectify the prejudicial and damaging atmosphere to which anonymous Internet defendants are subjected, four requirements must be diligently enforced: (1) courts must require complaints to comply fully with pleading rules, including those regarding propriety of jurisdiction and venue; (2) indications and allegations of counter-facts—particularly those that tend to destroy jurisdiction and venue—must be addressed early and with all due seriousness; (3) there must be fastidious observation of joinder rules, such that permissive joinder and dismissal can no longer be abused to the detriment of anonymous Internet defendants; and (4) effective notice must be given to putative defendants.

9. *See, e.g.*, Paul Cockerton, *Time to End Our Reliance on Unique Users*, PAUL COCKERTON (July 2, 2011, 5:41 PM), http://paulcockerton.wordpress.com/2011/07/02/time-to-end-the-reliance-on-unique-users/.

10. *See* Nathaniel Gleicher, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 323 (2008) ("From anonymous message boards criticizing massive corporations, to citizens who scrutinize elected officials, to websites that enable the anonymous release of government and corporate documents, the Internet has expanded the cape of anonymity to shield an army of pamphleteers.").

II. THE RIGHT TO SPEAK ANONYMOUSLY

An oft-quoted passage from *McIntyre v. Ohio Elections Commission*, explaining the justifications for anonymous speech, reads:

> Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.[11]

As the above passage suggests, there is a right to anonymity. This section will examine the justifications—constitutional, jurisprudential, and societal—supporting the right to be anonymous and the right to speak anonymously. Although these rights have long since been established,[12] a clear understanding of the scope and extent of their reach is necessary for proper understanding of the plight of the anonymous defendant, and the import of the rights that he or she is made to surrender under our current procedural scheme.

The Supreme Court cases that have discussed anonymous speech have for the most part noted that it has been protected because there is a valuable tradition in protecting speech.[13] Many cases note that famous authors and our Founding Fathers wrote anonymously to protect themselves from retribution, or simply to protect their privacy.[14] The Court has stated that "an author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment,"[15] and that "[a]nonymity is a shield from the tyranny of the majority."[16]

In many of these cases, dissenting jurists have pointed out that there should be no broad right to anonymity. For example, Justice Scalia in *McIntyre* stated that "[anonymity] facilitates wrong by eliminating accountability, which is ordinarily the very purpose of

11. *Anonymity*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/issues/anonymity (last visited Sept. 11, 2011) (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995)).

12. *See McIntyre*, 514 U.S. at 343.

13. *Id.*

14. *E.g.*, *id.*

15. *Id.* at 342.

16. *Id.* at 357 (citing JOHN STUART MILL, ON LIBERTY AND CONSIDERATIONS ON REPRESENTATIVE GOVERNMENT 1, 3–4 (R. McCallum ed. 1947)).

the anonymity."[17] Determining who is wrongfully avoiding accountability and who is rightly avoiding unfair retribution is difficult, but there should be some clear procedural rules to guide judges in determining when unmasking anonymous parties is fair game.

A. Anonymity as a Protection from Retaliation

Unpopular speech is always in great need of protection and anonymity. In *NAACP v. Alabama ex rel. Patterson*,[18] an Alabama corporations law required disclosure of membership lists of the NAACP.[19] In a unanimous decision, the Court stated that anonymity is tied to the rights of free speech and free association, and that, in this circumstance, disclosure would have a chilling effect.[20] The Court recognized that many residents of Alabama who normally would associate with the NAACP might not do so if their association was publicly known.[21] "[I]mmunity from state scrutiny of [Petitioner's] membership lists . . . is here so related to the right of the members to pursue their lawful private interests privately and to associate freely with others in doing so as to come within the protection of the Fourteenth Amendment."[22]

In *Talley v. California*,[23] a Los Angeles ordinance forbade anonymous posters and advertisements in an effort to curb false advertising, libel, and fraud.[24] Handbills were distributed that urged the boycott of several businesses and businessmen who did not offer equal employment opportunities to "Negroes, Mexicans, and Orientals."[25] The handbills had the address of "National Consumers Mobilization" printed on them but did not list any person's name.[26] Because the ordinance was not limited to offensive or obscene advertising and was not solely curbing fraud as it claimed, the Supreme Court held that it was an infringement of free speech.[27] There was no showing of a problem with libelous or

17. *Id.* at 385 (Scalia, J., dissenting).
18. 357 U.S. 449 (1958).
19. *Id.* at 451.
20. *Id.* at 466.
21. *Id.* at 462.
22. *Id.* at 466.
23. 362 U.S. 60 (1960).
24. *Id.* at 60–61, 64.
25. *Id.* at 61.
26. *Id.*
27. *Id.* at 64 ("[A]s in *Griffin*, the ordinance here is not limited to handbills whose content is 'obscene or offensive to public morals or that advocates unlawful

fraudulent handbills, so the ordinance was not narrowly tailored to protect speech.[28] However, the dissent noted that there was also no clear showing of a threat of retribution to the speakers.[29] The decision in *Talley* has paved the way for broad protection of anonymous speech because it can be assumed that in speech that criticizes, whether political or not, there is a potential for retribution, and an author has the right to protect his or her identity if he or she chooses.

In *Brown v. Socialist Workers '74 Campaign Committee,*[30] the Supreme Court carved out an exception for anonymous speech from the general rule on campaign contribution disclosures set out in *Buckley v. Valeo.*[31] The Court held that Ohio's campaign disclosure requirements could not constitutionally be applied to minor parties such as the Socialist Workers Party.[32] If either contribution or involvement was publicized, contributors and recipients would be subject to harassment and reprisals—specifically, those associated with the Socialist Workers Party feared that they would be fired or denied employment in the future.[33] This contrasts with the general rule of *Buckley* that the state interest in fair elections outweighs any need for anonymity in campaign contributions.[34]

The *Brown* case highlights the flexibility available for decisions involving political speech. When there is a risk of chilling speech because of retribution to speakers based on their views, there can and should be exceptions to protect those speakers with unpopular or minority viewpoints.

B. Anonymity and Compelled Identification in the Political Arena

The case that is most often cited for the proposition that there is a right to speak anonymously is *McIntyre v. Ohio Elections Commission.*[35] In 1988, Margaret McIntyre passed out leaflets that

conduct.' . . . Therefore we do not pass on the validity of an ordinance limited to prevent these or any other supposed evils." (quoting Lovell v. City of Griffin, 303 U.S. 444, 451 (1938))).

28. *Id.*
29. *Id.* at 69 (Clark, J., dissenting).
30. 459 U.S. 87 (1982).
31. 424 U.S. 1 (1976).
32. *Brown*, 459 U.S. at 101–02.
33. *Id.* at 99.
34. *Buckley*, 424 U.S. at 72.
35. 514 U.S. 334 (1995).

were meant to persuade people to vote against a school levy.[36] The leaflets were signed "CONCERNED PARENTS AND TAX PAYERS," and argued that the local school district had wasted money in previous levies and that "WASTE CAN NO LONGER BE TOLERATED."[37] Ohio law, at the time, prohibited anonymous political advertisements promoting a candidate or issue that would be decided in an upcoming election.[38] The scope of the law in *McIntyre* was narrower than the law in *Talley* because the Ohio law only applied to speech intended to influence the outcome of an election, and the alleged state interest was to prevent libel and fraud and provide the electorate with relevant information.[39]

The Court held that the exacting scrutiny standard was not met by the Ohio law.[40] When political speech is involved, any law that would restrict that speech must be narrowly tailored to a compelling state interest.[41] The majority also noted the great tradition of anonymous political speech as well as anonymous literature.[42] "The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse."[43] In a concurring opinion, Justice Thomas wrote that the text of the First Amendment must have been intended to protect anonymous speech at the time it was

36. *Id.* at 337.
37. *Id.*
38. *Id.* at 338. The applicable provision reads:

> No person shall write, print, post or distribute, or cause to be written, printed, posted or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to promote the nomination or election or defeat of a candidate, or to promote the adoption or defeat of any issue, or to influence the voters in any election, or make an expenditure for the purpose of financing political communications through newspapers, magazines, outdoor advertising facilities, direct mailings, or other similar types of general public political advertising, or through flyers, handbills, or other non-periodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes or is responsible therefor.

OHIO REV. CODE ANN. § 3599.09(A) (West 1988).
39. *McIntyre*, 514 U.S. at 344, 348.
40. *Id.* at 347.
41. *Id.*
42. *Id.* at 357.
43. *Id.*

written because many of the founders in fact practiced anonymous speech.[44] However, Justice Scalia's dissent noted that forty-nine states have laws that prohibit anonymous speech in campaigns, and there is nothing in the text of the Constitution that explicitly provides a right to anonymity.[45]

McIntyre has been one of the most-cited cases dealing with anonymity, and it contains at least two methods of looking at the question of anonymous speech. First, it notes that there is a tradition of protecting anonymous speech in our country.[46] This tradition is based on a deference given to authors to choose whether to identify themselves because that is a part of the message being conveyed, meaning that requiring identification is compelled speech.[47] The other method is to consider whether identification of an author will have an effect on whether the speech is made at all.[48] If self-identification is required, some may be less likely to speak, which would create an infringement of speech.[49]

In *Buckley v. American Constitutional Law Foundation*,[50] the Supreme Court struck down Colorado laws that required initiative-petitioners to be registered voters and to wear a name-badge stating whether they were paid or volunteer, and to provide a list of all paid workers.[51] Even though the petitioners would not be anonymous to those who knew them, the Court held that they had the right not to disclose their identities through identification badges.[52]

The right to be anonymous while publicly canvassing and promoting a cause has been reaffirmed in *Watchtower Bible v. Stratton*.[53] In that case, the Village of Stratton prohibited canvassing on residential properties without a permit.[54] Again, part of the decision rested on the right to maintain anonymity while exercising First Amendment rights.[55]

If the Supreme Court has made anything clear in its decisions

44. *Id.* at 358–61 (Thomas, J., concurring).
45. *See id.* at 385 (Scalia, J. dissenting).
46. *Id.* at 357.
47. *Id.* at 342.
48. *Id.*
49. *See id.* at 355.
50. 525 U.S. 182 (1999).
51. *Id.* at 186, 200.
52. *Id.* at 200.
53. Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150 (2002).
54. *Id.* at 154.
55. *Id.* at 167.

over the last half-century, it is that there is some protection for anonymity in the context of the First Amendment.[56] Of the Internet cases discussed below, few involve compelled disclosure, but rather a choice as to whether to allow an anonymous person to be identified after alleged wrongful acts have occurred.[57] Still, the Supreme Court cases discussed above can provide several helpful ideas about anonymity. Anonymity is to be protected when not doing so would impair the exercise of First Amendment rights.[58] Anonymity can be protected because compelling disclosure is equivalent to compelling speech, and there is a strong tradition of anonymous political speech that can be traced to our nation's founding.[59]

III. INEQUITABLE TREATMENT OF ANONYMOUS DEFENDANTS

This section will present the processes and procedures used to unmask anonymous defendants and will then explore the problems to which such practices give rise. These problems have persisted for some time,[60] and their net effect is the unfair and inequitable treatment of defendants who wish to remain anonymous.[61] Unfortunately, that disparity exists at nearly every stage in litigation, making it almost impossible for an anonymous defendant to retain his or her rights to privacy and anonymity.

At present, anonymous defendants are faced with several unique hurdles during litigation. For example, while an anonymous plaintiff who wishes to remain anonymous during the course of a suit is armed with the full repertoire of procedural tools necessary for full and vigorous litigation,[62] an otherwise anonymous

56. *See, e.g.*, *id.* at 167; Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

57. *See* discussion *infra* Part III.A.

58. *See, e.g.*, *Watchtower Bible,* 536 U.S. at 167.

59. *See, e.g.*, *McIntyre,* 514 U.S. at 357 ("Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.").

60. *See, e.g.*, Carol M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, 57 U. PITT. L. REV. 883, 885 (1996) (explaining that litigants in English courts began using pseudonyms more than three centuries ago).

61. *See id.* at 894–907.

62. *See, e.g.*, Aaron Morris, *Dude, Who's My Plaintiff?—Courts Allow Anonymous Plaintiffs*, BUS. L. ALERT (Dec. 1, 2008), http://www.businesslawalert.com/2008/12/articles/defamation/dude-whos-my-plaintiff-courts-allow-anonymous-plaintiffs/ ("On August 12, 2008, the Second District U.S. Court of Appeals reaffirmed the national and local trend toward recognizing a litigant's right to proceed

defendant seeking to protect that anonymity has his or her arsenal limited to motions to quash subpoenas seeking to discover information about his or her identity.[63] Furthermore, proceedings deciding whether to disclose the defendant's identity are instigated at the whim of the plaintiff, often in the improper forum, with inadequate service and notice, and with only the barest effort expended to ascertain whether the soon-to-be-identified defendant is the proper party against whom suit should be brought.[64] Moreover, the Federal Rules of Civil Procedure are largely silent or unclear on the matter of anonymous defendants,[65] leaving various jurisdictions to develop different methods for dealing with anonymous parties.[66] Unfortunately, although the difficulties facing anonymous defendants have long been known,[67] modern pleading and discovery rules remain inadequate to address and resolve these problems.[68]

A. How Anonymous Defendants Are Identified

Anonymous defendants come in varying degrees of anonymity. In BitTorrent[69] piracy cases, for example, defendants are often

anonymously through the courts.").

63. This is due to the procedural stage of the suit at the time when the defendant's identity is at risk of disclosure. Greater detail is provided in the discussion *infra* Part III.A. *See also Potential Legal Challenges to Anonymity*, CITIZEN MEDIA L. PROJECT, http://www.citmedialaw.org/legal-guide/potential-legal-challenges-anonymity (last updated Apr. 22, 2010) ("[Defendants] also have the legal right to contest a subpoena seeking to reveal [their] identity. [They] usually do this by filing a 'motion to quash' the subpoena . . . .").

64. *See* VPR Internationale v. Does 1–1017, No. 11-2068, 2011 U.S. Dist. LEXIS 64656, at *3 (C.D. Ill. Apr. 29, 2011) ("In this case, not a single one of the plaintiff's 1,017 potential adversaries has been identified. There is no adversarial process yet. Moreover, VPR ignores the fact that IP subscribers are not necessarily copyright infringers.").

65. *See, e.g.*, Call of the Wild Movie, LLC v. Does 1–1,062, 770 F. Supp. 2d 332, 341–45 (D.D.C. 2011) (discussing the issue of whether mass joinder of anonymous defendants is addressed by the Federal Rules of Civil Procedure).

66. *Compare* Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 445–56 (Md. 2009) (imposing stringent requirements prior to identification of anonymous individuals, including an assessment of the strength of the underlying defamation case), *with* Donkeyball Movie, LLC, v. Does 1–171, No. 10–1520 (BAH), 2011 WL 1807452, at *2–8 (D.D.C. May 12, 2011) ("[T]he putative defendant's First Amendment right to anonymity . . . is minimal and outweighed by the plaintiff's need for putative defendant's identifying information in order to protect its copyrights.").

67. *See, e.g.*, Rice, *supra* note 60, at 885.

68. *Id.* at 913–45.

69. BitTorrent is a popular peer-to-peer file sharing protocol, whereby files are broken into small pieces and distributed in such a way that recipients can

initially identified by an Internet Protocol (IP) address,[70] which is necessarily distributed to fellow users in order to facilitate file sharing. In other instances, such identifying information may be unavailable and the defendant may actually be truly anonymous.[71] Because the focus of this article is on the treatment of defendants who are at risk of identification, more attention will be given to those defendants that are less than fully anonymous.

Where some potentially identifying information is available, plaintiffs may use that information to name defendants pseudonymously, employing the discovery process to further identify defendants.[72] Often in the case of Internet defendants, the true identity of the party corresponding to the potentially identifying information can be obtained from a third-party online service provider (OSP), such as an Internet service provider (ISP), forum administrator, message board operator, e-mail provider, or online merchant.[73] Frequently, these OSPs record some amount of information to facilitate identification.[74] For example, an e-mail provider may log the IP address of the sender while the ISP that supplied that IP address records to which of its subscribers the IP address had been assigned.[75] Thus, through a bit of detective work, it may be possible to obtain the name and address for an online service user.[76]

---

often obtain them from fellow downloaders, rather than the source, thereby easing the burden on the original uploader. *See The Basics of BitTorrent*, BITTORRENT, http://www.bittorrent.com/help/manual/chapter0201 (last visited Sept. 9, 2011).

70. An IP address is a unique number assigned to each device on a network used to direct network traffic to and from the correct device. *IP Address Overview: The Basics on IP Addresses*, THE INTERNET DIG. (Oct. 25, 2004), http://www.theinternetdigest.net/articles/ip-address-overview.html. IP addresses are frequently provided by those who supply access to the Internet, known as internet service providers. *See id.*

71. *See* Roberto Aringhieri et al., *Fuzzy Techniques for Trust and Reputation Management in Anonymous Peer-to-Peer Systems*, 57 J. AM. SOC'Y FOR INFO. SCI. & TECH. 528, 529 (2006).

72. *See* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 390 n.2 (1971).

73. *See Information Stored by Third Parties*, SURVEILLANCE SELF-DEFENSE PROJECT, https://ssd.eff.org/3rdparties (last visited Sept. 10, 2011).

74. *See id.*

75. H.R. 1981, 112th Cong. § 4(h) (2011) ("A provider of an electronic communication service or remote computing service shall retain for a period of at least 18 months the temporarily assigned network addresses the service assigns to each account, unless that address is transmitted by radio communication (as defined in section 3 of the Communications Act of 1934).").

76. It may not be possible to accurately identify the proper plaintiff from the IP address alone, because multiple persons—authorized or not—may be sharing

In practice, first, the plaintiff sues a fictitious "John Doe."[77] The plaintiff then obtains the court's permission to subpoena identifying information from the relevant OSPs.[78] Once the plaintiff obtains such information from the OSPs, the plaintiff amends the complaint to name the person identified by the OSPs.[79] Frequently, the OSPs will notify the relevant person that the plaintiff is trying to obtain his or her information.[80] If the person whose identity is to be revealed objects to such disclosure, he or she is limited to filing a motion to quash the subpoena.[81] This is because he or she is technically not yet a party to the action,[82] and therefore does not have access to all the tools of litigation, such as motions to dismiss or for summary judgment.[83] In practice, this leaves a would-be defendant without any way to protect his or her privacy until it has already been invaded.

If the motion to quash is unsuccessful, the court may hold a hearing, during which the defendant can more fully oppose disclosure of his or her identifying information.[84] It should be

---

the same Internet connection. *See, e.g.*, Carolyn Thompson, *NY Child Pornography Case Underscores Wi-Fi Privacy Dangers*, AOL NEWS (Apr. 24, 2011), http://www.aolnews.com/2011/04/24/ny-child-pornography-case-underscores-wi-fi-privacy-dangers/ ("People who keep an open wireless router won't necessarily know when someone else is piggybacking on the signal, which usually reaches 300–400 feet . . . .").

77. Erik P. Lewis, Note, *Unmasking "Anon12345": Applying an Appropriate Standard When Private Citizens Seek the Identity of Anonymous Internet Defamation Defendants*, 2009 U. ILL. L. REV. 947, 954 (citing McMann v. Doe, 460 F. Supp. 2d 259, 262–63 (D. Mass. 2006)).

78. Donkeyball Movie, LLC v. Does 1–171, No. 10-1520 (BAH), 2011 WL 1807452, at *9 (D.D.C. May 12, 2011) ("To be clear, at this stage in the proceedings, the plaintiff is engaged in discovery to identify the proper defendants to be named in this lawsuit, including whether the exercise of jurisdiction over each potential defendant is proper.").

79. *See id.* at *1 (stating that the plaintiff had been given leave "to obtain identifying information for the putative defendants" because the defendants "were unidentified at the time the plaintiff filed its Complaint").

80. *See, e.g.*, *id.* (explaining that the court ordered the putative defendants' OSPs to send notices to them so the defendants could challenge the release of their information).

81. *Id.* at *9 ("If and when the putative defendant is ultimately named in this lawsuit, she will have the opportunity to file an appropriate motion challenging the Court's jurisdiction, and the Court will be able to evaluate her personal jurisdiction defense and consider dismissal. Until that time, however, dismissal under Rule 12(b)(2) is inappropriate." (citing London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 180–81 (D. Mass. 2008))).

82. *See* McMann v. Doe, 460 F. Supp. 2d 259, 266 (D. Mass. 2006) ("[T]his motion must be considered ex parte because John Doe is not known.").

83. *See Donkeyball Movie*, 2011 WL 1807452, at *8–9.

84. Lewis, *supra* note 77, at 954.

noted that this hearing is held in the court initially selected by the plaintiff when filing suit, which occurred before the plaintiff had ascertained the identity of the defendant;[85] thus, a host of defects with respect to jurisdiction, venue, and notice may exist.[86] These issues will be discussed later in this section.[87]

Courts have struggled to reach a consistent approach in deciding whether to allow plaintiffs to use discovery to identify the putative defendant.[88] Seeking to balance the interests of the plaintiff with those of the defendant and to provide opportunities for redress without "demand[ing] the court system unmask every insolent, disagreeable, or fiery anonymous online figure,"[89] two standards have emerged.[90] The more recent—and more exacting—of the two was put forth by the Delaware Supreme Court in its 2005 *Doe v. Cahill* decision.[91] The older standard was articulated by the Virginia Circuit Court in *In re Subpoena Duces Tecum to America Online, Inc.* in 2000.[92]

The *America Online* standard requires that the plaintiff have a "legitimate, good faith basis" for jurisdiction where the suit was filed, and that the identity of the putative defendant is necessary for litigation.[93] In contrast, the *Cahill* standard requires that: (1) the plaintiff must provide notice of his discovery request by replying to the original message; and (2) the plaintiff must support his claim with sufficient facts to overcome a motion for summary judgment.[94]

---

85. *Id.*

86. *See, e.g.*, *id.* (mentioning that if a plaintiff files in federal court based on diversity of citizenship, and the defendant, upon revealing himself, turns out to be a citizen of the same state as the plaintiff, then diversity is defeated).

87. *See infra* Parts III.B–C.

88. *See* Ryan M. Martin, Comment, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 U. CIN. L. REV. 1217, 1227 (2007) ("Courts . . . have applied different standards for determining whether an anonymous source should be unmasked . . . .").

89. *McMann*, 460 F. Supp. 2d at 266.

90. Lewis, *supra* note 77, at 954.

91. 884 A.2d 451 (Del. 2005)*; see also* Kevin McBride, *Discovery of Anonymous Online Speakers*, MCBRIDE L., PC (Mar. 8, 2011), http://www.mcbride-law.com /2011/03/08/discovery-of-anonymous-online-speakers ("The district court in the 9th Circuit matter on appeal applied the most exacting standard, established by the Delaware Supreme Court in *Doe v. Cahill.* The Cahill standard requires plaintiffs to be able to ***survive a hypothetical motion for summary judgment*** and *give, or attempt to give, notice to the speaker before discovering the anonymous speaker's identity.*") (citation omitted).

92. 52 Va. Cir. 26, 37 (2000), *rev'd in part on other grounds sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

93. *Id.*

94. *Cahill*, 884 A.2d at 461.

The *Cahill* court expressly rejected the *America Online* standard because "[*America Online*'s] 'good faith' standard is too easily satisfied to protect sufficiently a defendant's right to speak anonymously."[95] Legal commentators have also noted that neither the *America Online* court nor any other has ever explained how one satisfies the good faith basis requirement.[96] Given the difficulties involved in applying the *America Online* standard, courts have been employing the *Cahill* standard with greater frequency.[97]

Regardless of the standard applied, it appears that courts are generally willing to allow the plaintiff to proceed with expedited discovery so as to uncover the identity of the would-be defendant.[98] This trend appears to be slowing, however, with respect to cases with multiple anonymous Internet defendants—so-called "reverse class action" cases—such as in Internet piracy cases.[99] Although these cases are recent (within the past year and some currently undecided and subject to appeal),[100] several legal commentators suggest that such a shift may signal that the judiciary has come to understand the plight of the anonymous defendant.[101]

B. Issues with Pleadings

Initiating a case with one or more anonymous parties presents the problem of pleading unknown facts. For example, Rule 8(a)(1) of the Federal Rules of Civil Procedure requires that a pleading have "a short and plain statement of the grounds for the court's jurisdiction . . . ."[102] In the case of an anonymous

95. *Id.* at 458.

96. *See* Lewis, *supra* note 77, at 957–58 (citing Martin, *supra* note 88, at 1228); *see also* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 241 (Ct. App. 2008) ("[The good faith standard] offers no practical, reliable way to determine the plaintiff's good faith and leaves the speaker with little protection.").

97. *See, e.g.*, Mobilisa, Inc. v. Doe, 170 P.3d 712 (Ariz. Ct. App. 2007).

98. *See* Arista Records LLC v. Does 1–19, 551 F. Supp. 2d 1, 6 (D.D.C. 2008) (noting "the overwhelming number of cases where courts have . . . permitted expedited discovery in circumstances similar to the present.").

99. *See, e.g.*, VPR Internationale v. Does 1-1017, No. 11-2068, 2011 U.S. Dist. LEXIS 64656 (C.D. Ill. Apr. 29, 2011); Millennium TGA, Inc. v. Does 1-800, No. 10 C 5603, 2011 U.S. Dist. LEXIS 35406 (N.D. Ill. Mar. 31, 2011); IO Group, Inc. v. Does 1-435, No. C 10-04382 SI, 2011 U.S. Dist. LEXIS 14123 (N.D. Cal. Feb. 3, 2011).

100. *See, e.g.*, *VPR Internationale*, 2011 U.S. Dist. LEXIS 64656.

101. *See, e.g.*, Robert Z. Cashman, *Dead on Arrival—Judge Did Not Allow Plaintiff Attorneys to Subpoena the ISPs*, FED. COMPUTER CRIMES (May 3, 2011), http://torrentlawyer.wordpress.com/2011/05/03/john-doe-lawsuit-denied-expedited-discovery-no-access-to-isp-data/.

102. FED. R. CIV. P. 8(a)(1).

defendant, is it possible to plead ignorance or is it necessary to have a good faith basis for proceeding in a particular court? Recent file-sharing cases again provide examples of how courts have differing interpretations of the rules and their procedural effects.

Some courts have responded to a motion to dismiss for lack of personal jurisdiction by ruling that motions to dismiss are premature until an anonymous defendant is named and served, thereby allowing jurisdictional discovery.[103] However, in cases where an anonymous defendant is known by an IP address, it may be possible to approximately determine where the anonymous defendant is located. IP geolocation is the practice of determining a user's geographical location through their IP address, and has been available since 1999.[104] A few courts have now recognized that IP geolocation may provide sufficient information to indicate that jurisdiction and venue are not appropriate where the IP addresses appear to be coming from places outside the district where the case has been filed.[105]

The appropriate standard for pleadings should not have to change due to the presence of an anonymous party. In cases involving an anonymous party known only by a username, or with no facts suggesting geographical location, it may be appropriate to allow jurisdictional discovery in any district. However, at a minimum, a party should be required to plead a good faith reason to believe that, upon identification, the claims would survive a motion to dismiss.[106] Where a party knows only evidence that would contradict an allegation, such as the appropriateness of venue, jurisdictional discovery seems inappropriate.

---

103. *See, e.g.*, West Bay One, Inc. v. Does 1-1,653, 270 F.R.D. 13, 15 n.2 (D.D.C. 2010); London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153 (D. Mass. 2008); Virgin Records Am., Inc. v. Does 1-35, No. CIV.A. 05-1918(CKK), 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006).

104. *See* Stephanie Olsen, *Digital Envoy Wins Geotargeting Patent*, CNET NEWS (June 29, 2004), http://news.cnet.com/Digital-Envoy-wins-geotargeting-patent/2110-1032_3-5251844.html.

105. *See, e.g.*, Nu Image, Inc. v. Does 1-23,322, No. 11-cv-00301(RLW), 2011 WL 3240562, at *4 (D.D.C. July 29, 2011) ("Thus, the Court finds that the Plaintiff has a good faith basis to believe a putative defendant *may* be a District of Columbia resident if a geolocation service places his/her IP address within the District of Columbia, or within a city located within 30 miles of the District of Columbia. Without this threshold good faith showing, the Court finds Plaintiff's motion for expedited discovery inappropriate, as it would otherwise be based on Plaintiff's mere conjecture or speculation . . . .").

106. *See, e.g.*, *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 37 (2000), *rev'd in part on other grounds sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

C. *Abuses of Process*

In light of the disparity between courts and the inconsistent application of standards—or rather, the lack of a consistent standard—it comes as no surprise that anonymous defendants are subjected to various abuses under the current scheme. Under our justice system, anonymous Internet defendants are particularly vulnerable because their desire to retain their anonymity often compels them to strike unbalanced settlement agreements,[107] to refrain from responding to lesser abuses,[108] and to neglect to use the proper degree of discretion in seeking and retaining legal counsel.[109] Furthermore, in addition to the forum and notice deficiencies detailed in earlier sections,[110] problems of which the courts have long been cognizant, anonymous Internet defendants

107. *See, e.g.*, Eryk Salvaggio & Kurt Klappenbach, *File-Sharing Settlements Target 34 UMS Students*, THE MAINE CAMPUS (Nov. 19, 2007), http://mainecampus.com/2007/11/19/file-sharing-settlements-target-34-ums-students/ (discussing the impact of a bill that would link financial aid funding to a school's willingness to test technological deterrents to file-sharing, and noting that "[w]hile this bill is working through Congress, the RIAA announced that 417 pre-litigation settlement letters had been sent to college students nation-wide . . . ."); *see also* Nate Anderson, *P2P Lawyer: More Settlements Since Former-Lobbyist Judge's Ruling*, ARS TECHNICA L. & DISORDER (Apr. 12, 2011), http://arstechnica.com/tech-policy/news/2011/04/p2p-lawyer-more-settlements-since-former-lobbyist-judges-ruling.ars ("[M]ore anonymous P2P defendants are coming forward to settle."). *But see* David Kravets, *Settlement Rejected in 'Shocking' RIAA File Sharing Verdict*, WIRED THREAT LEVEL (Jan. 27, 2010, 2:47 PM), http://www.wired.com/threatlevel/2010/01/settlement-rejected-in-shocking-riaa-file-sharing-verdict/ ("'She is rejecting [the RIAA's settlement offer],' Joe Sibley, one of Thomas-Rasset's lawyers, said in a telephone interview. 'I think it proves our point. They want to use this case as a bogeyman to scare people into doing what they want, to pay exorbitant damages.'").

108. *See* Paul Alan Levy, *Litigating Civil Subpoenas to Identify Anonymous Internet Speakers*, 37 LITIGATION, no. 3, 2011 at 27, 30, *available at* http://www.citizen.org/documents/litigating-civil-subpoenas-to-identify-anonymous-internet-apeakers-paul-alan-levy.pdf ("[T]he most common response [if the defendant has hired a lawyer] on the part of the plaintiffs' lawyers is either to drop the case or to file no opposition [to the defendants' motions to quash]. . . . What this tells me is that these plaintiffs sought discovery to identify their critics without having any real intention of going forward with [their] . . . case.").

109. *See* David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3, 21 n.36 (2000) ("John Doe defendants do not have the option of appearing pro se for two reasons. First, a personal appearance would obviously negate a defendant's efforts to conceal his or her identity. Second, suits against John Does are frequently filed in jurisdictions distant to the defendants. As a result, anonymous defendants who wish to protect their identities are compelled to incur the expense of retaining counsel to represent them (assuming they are able to locate counsel in a distant jurisdiction on short notice).").

110. *See supra* Part III.B.

are saddled with additional procedural burdens and risks of less obvious harms. Given the anonymous nature of the defendants, plaintiffs are afforded a certain degree of freedom in the pleading and discovery processes that necessarily invades the privacy of would-be defendants after clearing notably low hurdles.[111]

One of the more pernicious forms of abuse inflicted by plaintiffs is the practice of voluntary dismissal, followed by additional joinder.[112] Under this practice, plaintiffs initially file suit against a large number of anonymous defendants, and provide notice through the defendants' OSPs.[113] Defendants can either wait until the plaintiff has availed itself of the discovery process and uncovered their identity, or take on an active role in the action. During this time, settlement offers are communicated from the plaintiff to the putative defendants.[114] These settlement offers typically demand that the defendant pay a sum of money, admit fault, and agree to refrain from repeating the behavior, in exchange for the plaintiff waiving his or her right to bring suit.[115] Once the plaintiff feels he or she has successfully reached as many settlement agreements as are likely, or if the current crop of defendants is particularly uncooperative, the plaintiff dismisses all but a handful of defendants, and joins many more, repeating the process.[116] In this way, the plaintiff is able to avoid aggregating filing fees and costs while reaching the greatest number of potential defendants (thereby accumulating the greatest amount of settlement payments).[117]

Particularly in mass file-sharing cases, plaintiffs have brought suit against a multitude of defendants, with the only rationale for the grouping being that the same copyrighted work was downloaded.[118] In these suits, the defendants were often from

111. *See supra* Part III.A.

112. *See, e.g.*, CP Productions, Inc. v. Does 1–300, No. 10 C 6255, 2011 WL 737761, at *1 (N.D. Ill. Feb. 24, 2011).

113. *See, e.g.*, *id.*

114. *See, e.g.*, *id.*

115. *See, e.g.*, *id.*

116. *See, e.g.*, *id.*

117. *See, e.g.*, *id.* ("No predicate has been shown for thus combining 300 separate actions on the cheap—if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees alone would have aggregated $105,000 rather than $350.").

118. *See, e.g.*, Boy Racer, Inc. v. Does 1–60, No. C 11–01738 SI, 2011 WL 3652521, at *1 (N.D. Cal. Aug. 19, 2011) ("Plaintiff claims that the Doe defendants illegally reproduced and distributed plaintiff's copyrighted creative work 'A Punk Rock Orgy in the Woods' . . . .").

different states, downloaded the file at different times and from different sources, and, in some instances, downloaded different files.[119] This would be analogous to joining separate and unrelated crimes committed by separate and unrelated criminals simply because the same model of television was stolen. Without a substantial factual nexus, joinder is clearly improper,[120] yet, because the technology is complex,[121] and due to the potentially high cost of bringing similar suits against possibly thousands of defendants,[122] courts have been willing to permit such joinder during the early stages of litigation.[123]

Another abuse visited upon anonymous defendants is the threat of identification and association with potentially embarrassing or shameful practices. For example, in *CP Productions, Inc. v. Does 1-300*, the alleged harm was the defendants' unauthorized downloading of a pornographic film titled "Cowgirl Creampie."[124] Many similar cases exist wherein the plaintiff uses the potentially embarrassing nature of the material downloaded to coerce settlement from the putative defendants who are at risk of being unmasked.[125] In situations like these, the plaintiff takes advantage of the considerable leverage afforded by the shame and humiliation that would be inflicted upon the defendant were he or

119. *Id.* at *3–4.

120. *See* FED. R. CIV. P. 20(a)(2) ("Persons . . . may be joined in one action as defendants if: (A) any right to relief is asserted against them jointly, severally, or in the alternative *with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences*; and (B) any question of law or fact common to all defendants will arise in the action.") (emphasis added).

121. *See* Call of the Wild Movie v. Does 1–1,062, 770 F. Supp. 2d 332, 345 (D.D.C. 2011) ("Given the administrative burden of simply obtaining sufficient identifying information to properly name and serve alleged infringers, it is highly unlikely that the plaintiffs could protect their copyrights in a cost-effective manner."); *This is How We Catch You Downloading*, TORRENTFREAK (Apr. 14, 2007), http://torrentfreak.com/this-is-how-we-catch-you-downloading/ (detailing a process used to trace users connecting to P2P networks).

122. *See, e.g.*, *CP Productions*, 2011 WL 737761, at *1 ("[I]f CP had sued the 300 claimed infringers separately . . . the filing fees alone would have aggregated $105,000 rather than $350.").

123. *See, e.g.*, VPR Internationale v. Does 1–17, No. C 11-01494 LB, 2011 WL 1465836, *1–3 (N.D. Cal. Apr. 15, 2011).

124. 2011 WL 737761, at *1.

125. *See* Liberty Media Holdings, LLC v. Colo. Members of Swarm of Nov. 16, 2010 to Jan. 31, 2011, No. 11-cv-01171-WYD-KMT, 2011 WL 1812654, at *1–2 (D. Colo. May 12, 2011) (permitting discovery for the purpose of identifying defendants who allegedly downloaded gay pornography); *see also* Nate Anderson, *Meet Evan Stone, P2P Pirate Hunter*, ARS TECHNICA L. & DISORDER (Feb. 7, 2011), http://arstechnica.com/tech-policy/news/2011/02/meet-evan-stone-p2p-pirate-hunter.ars.

she to be associated with the allegedly infringed content. The defendant has a strong incentive to settle in order to retain anonymity—often accepting an otherwise disadvantageous offer—even when he or she may have otherwise emerged victorious from litigation.

A third form of abuse takes advantage not of the anonymous defendants, but of the third parties.[126] Because third-party ISPs can be compelled by subpoena—indeed, most Internet service providers will refrain from disclosing subscriber information absent a court order[127]—to assist in ascertaining the identity of those associated with identifying information such as IP addresses, ISPs may suffer a significant burden in assisting litigation for which they have no interest in the outcome. Particularly where hundreds of potential defendants are listed, ISPs may have to expend considerable time, resources, and manpower to provide the plaintiff with the requested information, as well as notify those whose information is at risk of disclosure.[128] The use of the discovery process in this way pits the ISPs against their customers for the benefit of a party with whom the ISP may have had no previous association.[129] Additionally, where plaintiffs have done little or nothing to determine the propriety of jurisdiction with

126. *See, e.g.*, Jacqui Cheng, *NFL Fumbles DMCA Takedown Battle, Could Face Sanctions*, ARS TECHNICA UPTIME (Mar. 20, 2007), http://arstechnica.com/business/news/2007/03/nfl-fumbles-dmca-takedown-battle-could-face-sanctions.ars (discussing the National Football League's abuse of the Digital Millennium Copyright Act takedown provisions by sending repeated takedown requests regarding the same content).

127. Becky Waring, *ISPs Assist in Cutting Off File-Sharing Users*, WINDOWS SECRETS (May 7, 2009), http://windowssecrets.com/top-story/isps-assist-in-cutting-off-file-sharing-users ("[M]ost ISPs in the U.S. and other countries will release information about subscribers only when presented with a court order . . . ."); *see also* Office of Student Conduct, *Peer-to-Peer File Sharing*, U. OF PENNSYLVANIA OFF. OF STUDENT CONDUCT, http://www.upenn.edu/osc/pages/file_sharing.html (last visited Sept. 9, 2011) ("[M]any ISPs will not share subscriber information with copyright owners . . . .").

128. *See* Evan Brown, *Internet Law in the Courts*, 14 J. INTERNET L. 32, 32–33 (2011) ("Prosecuting a case against thousands of copyright infringement defendants is an enormous task, both for the plaintiffs' attorneys as well as the ISPs who must respond to the subpoenas. Having so many defendants risks making the case unmanageable.").

129. *See In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26, 32 (2000) *rev'd in part on other grounds sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001) ("If AOL did not uphold the confidentiality of its subscribers, as it has contracted to do, absent extraordinary circumstances, one could reasonably predict that AOL subscribers would look to AOL's competitors for anonymity. As such, the *subpoena duces tecum* at issue potentially could have an oppressive effect on AOL.").

respect to its multiple defendants, the sting of this abuse is compounded by the fact that much of the ISP's efforts and expenses may be for naught.

The fourth type of abuse is the use of court proceedings to identify a defendant where no legitimate claim exists.[130] A plaintiff can bring a false or tenuous claim solely for the purpose of identifying the defendant, dropping the claim after the defendant is called out.[131] Such suits may have a chilling effect on otherwise free speech merely because those at risk of such suits are unwilling or unable to expend the time and resources to defend against allegations, however meritless.[132] Indeed, some litigants have employed this strategy so successfully and so frequently as to have such behavior lambasted in popular media.[133]

A final form of abuse is the result of inadequate notice. While some case law supports a notice requirement,[134] other cases are silent on the matter.[135] Furthermore, even in those instances where notice is required, such notice is often insufficient.[136] For example, the *Dendrite International, Inc. v. Doe No. 3* notice requirement is as follows:

> We hold that when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts

130. Levy, *supra* note 108, at 3 (discussing how plaintiffs seek discovery to identify their critics without having any real intention of going forward with their case).

131. *Id.*

132. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

133. *See South Park: Trapped in the Closet* (Comedy Central television broadcast Nov. 16, 2005), *available at* http://www.southparkstudios.com/full-episodes/s09e12-trapped-in-the-closet.

134. *See* Mobilisa, Inc. v. Doe, 170 P.3d 712, 721 (Ariz. Ct. App. 2007); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 244 (Ct. App. 2008); Doe v. Cahill, 884 A.2d 451, 460 (Del. 2005); Solers, Inc. v. Doe, 977 A.2d 941, 954 (D.C. 2009); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

135. *See, e.g.*, *In re* Subpoena Duces Tecum to Am. Online, Inc., 52 Va. Cir. 26 (2000) *rev'd in part on other grounds sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

136. *See* Matthew Nied, *Protecting Internet Anonymity: The Case for Providing Notice to Anonymous Defendants in Defamation Cases*, L. IS COOL (Nov. 9, 2009), http://lawiscool.com/2009/11/09/protecting-internet-anonymity-the-case-for-providing-notice-to-anonymous-defendants-in-defamation-cases.

> should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board.[137]

Given the plaintiff's lack of reliable identifying information for the defendant, the *Dendrite* court required only that the plaintiff provide indirect notice, by posting a message on the "pertinent message board."[138] Unfortunately, there is no guarantee that anonymous defendants will check—or indeed, are even aware of the existence of—such message boards. As a result, a would-be defendant may receive no notice of the proceedings in which his or her privacy is at risk.

D. Third-Party Reactions When Subpoenaed

Most ISPs or website operators have little motivation to either comply with a request to identify anonymous speakers (outside of a duty to respond to a subpoena) or to use their resources in protecting anonymous speakers. Some ISPs have had subpoenas seeking the identities of anonymous parties successfully quashed,[139] or have been granted additional time to respond.[140] However, these motions were apparently filed for the benefit of the ISPs, and it would not be reasonable to assume that an ISP will file a motion to quash a subpoena in most cases. An ISP may simply have nothing to gain from costly legal defense.

Additionally, website operators have very little risk of liability for most tort claims that would arise out of content created by an anonymous third party because section 230 of the Communications Decency Act shields them from such tort liability.[141] This law has been read broadly enough in some circumstances so that a website cannot be required to remove content even after a court has found that content to be defamatory.[142] Further, a website does not have a

137. *Dendrite*, 775 A.2d at 760.

138. *Id.*

139. LFP Internet Grp., LLC v. Does, No. 10-MC-122, 2011 U.S. Dist. LEXIS 5534, at *3 (D.S.D. Jan. 20, 2011) (granting Midcontinent Communications, Inc.'s motion to quash).

140. *See* Achte/Neunte Boll Kino Beteiligungs GMBh & Co. KG v. Does 1-4, 577, No. 10-453 (RMC), 2010 WL 4905811, at *1 (D.D.C. Nov. 19, 2010) (granting plaintiff's motion for additional time to name and serve defendants while waiting for information from ISPs).

141. 47 U.S.C. § 230 (2011). In particular, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* at (c)(1).

142. Blockowicz v. Williams, 675 F. Supp. 2d 912, 914–15 (N.D. Ill. 2009), *aff'd*, 630 F.3d 563 (7th Cir. 2010) (holding that internet website hosts could not be

duty to keep records in order to obtain protection under section 230, though some legal scholars have recommended that adequate record keeping be required in order to receive such immunity.[143] If the ISP or website operator cannot be sued, and has no useful records to subpoena, a valid case may go nowhere against an anonymous defendant.

IV. RECOMMENDATIONS

Although the authors do not propose complete solutions to these problems, the following recommendations are offered as potential improvements that may alleviate some of the harm inflicted on anonymous Internet defendants as a result of our current system.

First, each part of the complaint—including jurisdiction and venue—should be well-plead. Rather than a simple recitation that "jurisdiction is believed to be proper," plaintiffs bringing suit against anonymous defendants should be required to plead some facts as to why jurisdiction is proper. Functionally, parties should be required to assert facts that tend to show the propriety of their jurisdiction and venue selections.

One possible method of doing so would be for plaintiffs to use IP geolocation. Although still far from perfect, modern geolocation is often accurate to approximately twenty-two miles,[144] and new techniques are emerging which are accurate to approximately four-tenths of a mile.[145] While twenty-two miles may not be enough to personally identify the user associated with a specific IP address, it should oftentimes be sufficient to determine proper jurisdiction and venue. Given the simplicity and negligible expense involved with this practice,[146] the burden added by

forced to remove defamatory statements from their sites when the host is not a party in the action); *see also* Mike Masnick, *Two Courts Disagree on Whether or Not a Website Can Be Forced to Remove User-Created Defamatory Content*, TECHDIRT (Jan. 4, 2011, 4:30 AM), http://www.techdirt.com/articles/20110102/00241112482/two-courts-disagree-whether-not-website-can-be-forced-to-remove-user-created-defamatory-content.shtml (explaining the decisions).

143. *See* David Thompson, *Fixing the CDA 230 Subsidy While Preserving Online Anonymity*, THE VOLOKH CONSPIRACY (June 10, 2010, 8:33 PM), http://volokh.com/2010/06/10/fixing-the-cda-230-subsidy-while-preserving-online-anonymity/.

144. YONG WANG ET AL., TOWARDS STREET-LEVEL CLIENT-INDEPENDENT IP GEOLOCATION 1 (2011), *available at* http://www.usenix.org/event/nsdi11/tech/full_papers/Wang_Yong.pdf.

145. *Id.* at 1–2.

146. *See Lookup IP Address Location*, WHATISMYIPADDRESS.COM, http://

requiring that plaintiffs take this small affirmative step is marginal and far outweighed by the assurance that most anonymous defendants will be subjected to suit only where jurisdiction and venue exist, thus saving both judicial and party resources.

A second, related improvement would be to take seriously all indications of counter-facts. Presently, courts often ignore the anonymous defendant's assertion that jurisdiction or venue is improper,[147] and instead permit the plaintiff to proceed with limited discovery for the purpose of determining the putative defendant's identity (thus enabling the jurisdictional inquiry).[148] Similarly, some plaintiffs have continued to press for disclosure of identity even where facts, such as IP geolocation results, IP addresses belonging to ISPs that do not offer services within the district, or out-of-state letters from the would-be defendants' attorneys asserting that jurisdiction is improper strongly suggest that jurisdiction or venue may be improper.[149] Prohibiting plaintiffs from proceeding where there are clear indications of jurisdictional defects would save both judicial and party resources and help to ensure that the proper court hears the matter. It would also limit the kinds of strategic abuse detailed in earlier sections[150] and discourage parties who would be tempted to engage in such practices by requiring them to make a good faith inquiry where such indications are present.

Third, rules of joinder must be fastidiously observed in cases with multiple anonymous Internet defendants. Courts must cease to permit joinder in cases where traditionally required elements, such as common instrumentalities, shared time and place, or concerted efforts are conspicuously absent. Again, a more robust, fact-based pleading requirement would serve to limit joinder in cases where joining separate and distinct defendants would normally be improper.

Fourth, notice requirements must be improved to guarantee that putative defendants receive actual notice of proceedings

whatismyipaddress.com/ip-lookup (last visited Sept. 18, 2011) (providing a tool designed to give additional information for specific IP addresses).

147. *See, e.g.*, Donkeyball Movie, LLC v. Does 1–171, No. 10-1520 (BAH), 2011 WL 1807452, at *4 (D.D.C. May 12, 2011) (holding that joinder "of unknown parties identified only by IP addresses is proper" under Rule 20(a)(2) of the Federal Rules of Civil Procedure).

148. *See id.* at *4–7 (finding joinder proper at the early stage of litigation, even where movant's assertion of misjoinder may be meritorious).

149. *Id.*

150. *See supra* Part III.C.

concerning their privacy. One possible way to ensure that those involved receive notice would be to create a formal requirement for OSPs to provide such notice to their subscribers. Unfortunately, such a process would rely on uninvolved and disinterested third parties, which may not be enough to safeguard the rights of would-be defendants. However, because plaintiffs often lack the ability to contact defendants directly,[151] such notice and identity escrow may be necessary if effective notice is to be given.

Finally, whatever procedural standards are applied to unmasking anonymous defendants they should be applied equally to different causes of action. Two anonymous defendants with equally strong or weak cases, one accused of copyright infringement and the other defamation, should have the same odds of success on procedural matters. Neither copyright infringement nor defamation is protected speech, but if the plaintiff cannot succeed in proving its case, both defendants may be equally harmed by being identified.

V. CONCLUSION

None of the proposals from the foregoing section are novel; all of the suggested methods are currently being employed by various courts to resolve the very problems outlined in this article.[152] The problem, then, is lack of unity. Where one court requires detailed facts in order to assert jurisdiction in cases involving anonymous defendants,[153] another allows the plaintiff to proceed with identity-related discovery before addressing the question of jurisdictional propriety.[154] Because the Internet spans the entire nation,[155] the

151. By their very nature, anonymous defendants are unknown, and thus lack contact information.

152. *See, e.g.*, Boy Racer, Inc. v. Does 1–22, No. 11 C 2984, 2011 U.S. Dist. LEXIS 49557, at *1–2 (N.D. Ill. May 9, 2011) ("Steele and his client [should] pursue the normal path of suing an identifiable (and identified) defendant or defendants rather than a passel of 'Does.'. . . Boy Racer is free to advance its copyright infringement claims against one or more identified defendants on an individual basis or, if appropriate, a plausible conspiracy theory."); CP Productions, Inc. v. Does 1–300, No. 10 C 6255, 2011 WL 737761 (N.D. Ill. Feb. 24, 2011) (upholding previous order "dismissing the action without prejudice against all 300 putative defendants" under Rule 4(m) of the Federal Rules of Civil Procedure); Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001) ("[T]he plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.").

153. *Dendrite Int'l, Inc.*, 775 A.2d at 760–761.

154. *See, e.g.*, Donkeyball Movie, LLC v. Does 1–171, No. 10-1520 (BAH), 2011

law applied to the particular case—and therefore, the amount of protection afforded to the defendant's privacy—varies by the state in which the plaintiff files suit, thereby encouraging forum shopping. Exacerbating this problem is the fact that many of the lawsuits brought against anonymous Internet defendants (e.g., file-sharing and copyright infringement) have their cause of action established by federal law, giving the plaintiff some leeway to pick and choose among the courts to select one that is unsympathetic to the privacy concerns of anonymous Internet defendants.[156]

In light of the nationwide nature of the Internet, any solution must be nationwide, as well. Unfortunately, state sovereignty makes it difficult for different jurisdictions to reach a consensus, but as states recognize the abuses inflicted upon anonymous Internet defendants, they may come to adopt the solutions already found by others. National agreement on measures designed to protect the identities of anonymous Internet users that still affords plaintiffs opportunities to unmask their opponents where genuine disputes exist would go a long way towards leveling the playing field.

WL 1807452 (D.D.C. May 12, 2011).

155. *See* Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOC'Y, http://www.isoc.org/internet/history/brief.shtml (last visited Sept. 1, 2011).

156. At the time of writing, courts in the District of Columbia have tended to fall in this category. *See, e.g.*, *Donkeyball Movie*, 2011 WL 1807452.