UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 81 | Number 3 Article 6

3-1-2003

And the I(SP)s Have It...But How Does One Get It - Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation

Megan M. Sunkel

And the I(SP)s Have It . . . But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation

INTRODUCTION

Fraud, hacking, child pornography, and illegal gambling are but a few of the crimes that are just a mouse-click away from a knowledgeable computer user.[1] The fact that millions of people use the Internet today[2] provides ample opportunity for similar civil wrongs, including defamation. Companies increasingly are becoming

1. The Internet is an international network of computers providing its users with a plethora of communication methods. Reno v. ACLU, 521 U.S. 844, 849–52 (1997). These communication forums are collectively known as "cyberspace"—an accessible medium without a geographical location. *Id.* at 851. For a background discussion of the Internet and its unique potential as a communication environment, see *id.* at 849–53. For an excellent discussion on Internet crimes in general, see generally Laura J. Nicholson et al., *Computer Crimes*, 37 AM. CRIM. L. REV. 207 (2000) (tracking developments in computer-related criminal law and legal literature) and *infra* note 18 and accompanying text.

2. *Infra* note 20 and accompanying text.

the victims of online defamation.[3] Such online defamation is potentially devastating as companies' reputations are often linked to the prices of their stock.[4] The problem is so acute, in fact, that at least one corporation has emerged to provide a 'watchdog' service, scouring the Internet for negative comments that defame its corporate clients.[5] Finding these defamatory statements, however, is just the beginning of a long, uphill battle for injured companies.

Since Congress has taken away any opportunity to hold the online publishers liable for the defamatory statements of their users,[6] a company's only recourse is to directly sue the writers of the material. Many computer users operate under pseudonyms, however, masking their true identities.[7] This cloak of anonymity—part of the First Amendment's right to free speech[8]—combined with a lack of standards for these online cases, make seeking relief for defamation in cyberspace unnecessarily difficult.

This Comment explores the many difficulties a company confronts in pursuing an Internet defamation suit, particularly overcoming a motion to quash a subpoena when the identity of the author is unknown. Part I discusses the tort of defamation both in a general context and then as it uniquely applies to Internet discourse. Part II addresses the potential problems of suing unknown defendants, including a discussion of the ineptness of the Federal Rules of Civil Procedure in dealing with "John Doe" defendants. Part III surveys courts' attempts to create a standard for handling Internet defamation lawsuits and the inconsistent results in Internet defamation cases. Finally, Part IV explores one possible solution to the lack of standards in these cases by comparing subpoenas in Internet defamation cases to civil lawsuits involving reporters or journalists. The competing interests that arise in seeking a reporter's disclosure of sources are very similar to those arising in Internet

3. *See* Tom Collins, *As CyberSlander Suits Grow, Free Speech Threatened*, FULTON COUNTY DAILY REP., July 2, 2001, at 1.

4. One commentator has called "the potential impact a cybersmear campaign can have on a corporation's reputation or its stock prices," devastating. Nicole B. Casarez, *Dealing with Cybersmear: How to Protect your Organization from Online Defamation*, 47 PUB. REL. Q. 40, 40 (2002).

5. Cyveillance is a Virginia-based company and one of its services is to search the Internet for its corporate customers, looking for slanderous writings. Collins, *supra* note 3.

6. *Infra* notes 49–55 and accompanying text.

7. *See infra* notes 24–26 and accompanying text.

8. The Supreme Court has held that the right to speak anonymously has been an important part of speech throughout history and is protected by the First Amendment. Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 199 (1999); McIntyre v. Ohio Elections Comm., 514 U.S. 334, 341 (1995); Talley v. California, 362 U.S. 60, 64–65 (1960).

defamation cases, and thus the courts' standards in these cases could provide some much needed guidance.

I. THE TORT OF DEFAMATION

A. *Defamation Traditionally*

Although the First Amendment protects the right to free speech, some speech is of such little value to society that the First Amendment offers it no protection.[9] The Supreme Court has identified one such exception in the tort of defamation.[10] A word or statement is defamatory[11] if it tends to harm the reputation of another person or entity.[12] In a legal action for defamation, whether a statement is capable of being defamatory is a question of law,[13] whereas whether the statement is both false and understood as defamatory by its audience are questions of fact.[14] In reaching the factual determinations, the fact-finder examines the allegedly defamatory statement in the total context in which it appeared and in light of the surrounding circumstances.[15]

A defendant has available two possible defenses to a claim of defamation: (1) that the defendant is a public figure; or (2) that the defendant's statement was merely her opinion.[16] If the defendant successfully pleads one of these defenses, the plaintiff must satisfy a more rigorous standard—i.e., the plaintiff must demonstrate "actual

9. Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942) ("[I]t is well understood that the right of free speech is not absolute at all times and under all circumstances.").

10. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 268–72 (1964); Gertz v. Robert Welch, Inc., 418 U.S. 323, 340–41 (1974). Defamation can occur by either written or oral communication. If the statements are written it is called libel, while defamatory oral statements are called slander. BLACK'S LAW DICTIONARY 927 (7th ed. 1999) (defining libel as "[a] defamatory statement expressed in a fixed medium, esp. writing"). This Comment explores only libelous statements, but will use the general phrase "defamation" to describe this tort.

11. There is no list of defamatory words; each case is a unique question of facts. Babb v. Minder, 806 F.2d 749, 758 (7th Cir. 1986) (citing Korbar v. Hite, 43 Ill. App. 3d 636, 639 (1976) ("There is no general rule defining what words are defamatory and, therefore, each case depends upon its own facts.").

12. RESTATEMENT (SECOND) OF TORTS § 559 (1977) ("A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."). Defamation is a state law tort, so the definition varies between jurisdictions. *Sullivan*, 376 U.S. at 256.

13. Dilworth v. Dudley, 75 F.3d 307, 309 (7th Cir. 1996).

14. Baker v. Warner, 231 U.S. 588, 594 (1913).

15. Cox Enter., Inc. v. Bakin, 426 S.E.2d 651, 653–54 (Ga. App. 1992).

16. *Sullivan*, 376 U.S. at 282–83 (creating the then-controversial "public official" exception to defamation).

malice" on the part of the defendant.[17] Though some commentators argue that Internet discourse should fit into one of these two exceptions,[18] thereby warranting the heightened burden, these commentators fail to appreciate, as this Comment will clarify, the unique concerns that pursuing a claim of Internet defamation presents.

B. *Defamation on the Internet*

Defamation on the Internet provides an original twist to some of the existing issues of defamation law. Defamation on the Internet is unique for several reasons: (1) as a publication medium, the Internet is unique; (2) the consequences of defamation actions resulting from online communications can be different; and (3) determining the proper defendant often will be difficult.

1. The Internet as a Publication Medium

Though one may argue that the Internet should not be treated as a separate medium in the eyes of the law, there are many reasons that, as a vehicle of speech, the Internet stands alone. First, the Internet, as an unparalleled store of information, is a unique publication medium, comprised of billions of publicly available pages canvassing the spectrum of various information.[19] One reputable surveyor estimates that over five hundred million people worldwide are Internet users.[20]

---

17. In *N.Y. Times Co. v. Sullivan*, the Court held that for a public figure to prevail in a defamation action, he must prove the defendant acted with actual malice, thus increasing the standard from negligence. *Id.* at 280.

18. *See* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Disclosure in Cyberspace*, 49 DUKE L.J. 855, 865 (2000) (arguing that these cases should fall into the opinion exception); Jeremy Stone Weber, Note, *Defining Cyberlibel: A First Amendment Limit for Libel Suits Against Individuals Arising from Computer Bulletin Board Speech*, 46 CASE W. RES. L. REV. 235, 277 (1995) (arguing that the subjects of Internet discussion should be considered public figures). One California judge agreed, holding that the defendants in an Internet libel case were not liable because they were stating their opinion, and therefore, the audience could not consider this libel. Global Telemedia Int'l v. Doe, 132 F. Supp. 2d 1261, 1270 (C.D. Cal. 2001).

19. Press Release, Cyveillance, Internet Exceeds 2 Billion Pages (July 10, 2000), *at* http://www.cyveillance.com/web/us/newsroom/releases/2000/2000-07-10.htm (on file with the North Carolina Law Review) (stating the current size of the Internet in web pages and predicting that at the current, booming rate of expansion, as of early 2001 the size of the Internet should be doubled—to four billion pages).

20. NEILSON NET RATINGS, HOW MANY ONLINE? (Aug. 2001), *at* http://www.nua.ie/surveys/how_many_online/index.html (on file with the North Carolina Law Review).

In addition to its enormity, the Internet provides a limitless array of opportunities to its users.[21] The Internet, through various chat rooms and bulletin boards, provides users with the prospect of discussion on virtually every possible subject. Nearly every publicly traded corporation, for example, has at least one Web site dedicated to covering the corporation's activities and permitting ordinary users to publicly express their opinions or concerns regarding the corporation.[22] As one commentator explained, "[the Internet] empowers ordinary individuals with limited financial resources to 'publish' their views on matters of public concern."[23] Not only do these forums have a potential audience of millions, but Internet posters are further inspired to speak freely because they are able to do so anonymously.[24] David Sobel, an attorney for the Electronic Privacy Information Center, asserts that communicating anonymously is one of the Internet's greatest appeals.[25] Yet this attraction may come at a high price, as users, hidden behind a cloak of anonymity, speak without fear of the consequences.[26]

Another interesting characteristic of the Internet as a public discussion forum is the questionable reliability of its content. Though some commentators argue that visitors to web bulletin boards realize

21. The Supreme Court explained this opportunity, stating that with the Internet, "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox." Reno v. ACLU, 521 U.S. 844, 870 (1997).

22. These sites, which may be run by the company, its investors, or outsiders, range in subject from stock prices and potential profits to rumors of infidelity by the corporate officers. The postings contain "information, misinformation, rumor, speculation and strongly stated opinions" on the companies, and while these conversations used to occur around a water cooler, today they are heard by thousands, if not millions, of listeners. DONNA DEMAC, CYBERSMEARS AND CONSUMER REVENGE DOT COM: CORPORATE THREATS TO ONLINE FREE SPEECH (National Coalition Against Censorship, Aug. 2000), *at* http://www.ncac.org/issues/cybersmears.html (on file with the North Carolina Law Review).

23. Lidsky, *supra* note 18, at 860 (discussing how the Internet gives a powerful voice to the ordinary user).

24. *See* Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, 1530 (1996) (discussing the benefits of open discourse in cyberspace on topics such as sexual abuse or unpopular political ideas that may not be discussed if it were not for pseudonyms).

25. Rebecca Fairly Raney, *Judge Rejects Online Critic's Efforts to Remain Anonymous*, N.Y. TIMES, June 15, 1999, *at* http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html (on file with the North Carolina Law Review). *See generally* David Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3 (2000) (discussing Internet anonymity).

26. Lidsky, *supra* note 18, at 863 (explaining that Internet users have a heightened sense of "anything goes" because of the use of pseudonyms).

that most of what they read is unsubstantiated gossip,[27] others suggest that people do believe what they read online, perhaps relying on this information in making their own personal financial decisions.[28] Regardless of this debate, that the Internet is a powerful means for disseminating news and opinion—one that has a significant potential to harm the reputation of corporations subject to this online criticism—is undisputed.[29] On the other hand, the Internet, and more specifically Internet message boards, offer allegedly defamed entities a unique opportunity to combat the defamatory comments by instantly replying to defend themselves or their reputations at no cost.[30]

2. The Consequences of Online Defamation

The potential consequences of Internet defamation further distinguish this subset of defamation cases. In analyzing this distinctive characteristic of Internet defamation cases, courts and commentators should first consider the motive or goal of a corporation that files the suit and then assess the potential "chilling effect" that such suits could have on free speech, particularly on Internet discourse.

Defamation suits involve three types of damages: (1) special damages for "the loss of something having economic or pecuniary value;"[31] (2) presumed damages—a common law term allowing for compensation for harm of unquantifiable amounts; and (3) punitive

---

27. Joshua R. Furman, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation*, 25 SEATTLE U.L. REV. 213, 217 (2001) (alleging that most users know to take what they read online "with a grain of salt" because its validity cannot be verified and declaring there is a growing understanding that the Web bulletins are of questionable factual value).

28. Bob Cook, *Down and Dirty: Phycor and Other Companies Sue Anonymous Message Posters for Internet Mudslinging*, MODERN PHYSICIAN, June 1, 1999, at 30 (stating that although these message boards were originally "laughed off," companies are now taking them much more seriously as they are being confronted about the online rumors by employees and investors; furthermore, day traders are using the information available on web bulletins to make stock decisions).

29. Lidsky, *supra* note 18, at 863 (describing Internet communication as "a medium more pervasive than print," with tremendous power to injure reputations).

30. Memorandum In Support of Motion of J. Doe to Quash Subpoena Issued to Silicon Investor/Infospace, Inc., Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001) (No. C01-453Z). Furthermore, as one commentator noted, if online comments are driving stock prices down, the company has the same opportunity as those writing the negative comments to get online and attempt to inflate its demand with more positive ones. DEMAC, *supra* note 22.

31. Matherson v. Marchello, 473 N.Y.S.2d 998, 1000 (N.Y. App. Div. 1984) (quoting RESTATEMENT (SECOND) OF TORTS § 525 cmt. B (1977)).

damages, which are granted only upon a showing that the defendant wantonly injured the plaintiff.[32] Most likely, a corporate defendant will not file a defamation suit hoping to receive monetary compensation.[33] Corporations, instead, file in hopes of either identifying the unknown speaker,[34] who is likely an employee of the corporation she is defaming, or eliminating the existence of these online remarks.[35] In *Raytheon Co. v. John Does 1–21*,[36] for example, Raytheon voluntarily dismissed its suit immediately upon learning the identity of its defendants, who were Raytheon employees.[37] This dismissal may not be a break for the defendants, however, since they may now face losing their job or incurring other reprimands from their employer.

Other than the damage awards that an individual plaintiff may recover, Internet defamation suits potentially have farther-reaching consequences. Like so many other First Amendment issues, online defamation suits could have devastating effects on our freedom of speech. The theory is that defamation suits discourage speakers from talking, even behind the cloak of a pseudonym, for fear of the

32. For a discussion of these damages, see Michael Hadley, Note, *The* Gertz *Doctrine and Internet Defamation*, 84 VA. L. REV. 477, 480–81 (1998).

33. Typically, the defendants in these suits would be incapable of fulfilling a large monetary award; the incentive to litigate is thus very different for corporate clients. *See* Lidsky, *supra* note 18, 867–77 (discussing the non-monetary incentives that companies have in pursuing defamation litigation against anonymous defendants). Most companies treat potential litigation like any other business decision, analyzing the costs and the benefits. *See id.* at 876–83 (examining the possible reasons that a corporation may sue a "John Doe" for defamation, and arguing that, although corporations may never see a dime from the defendants, corporations may nonetheless "deem it economically rational to sue the pseudonymous posters who make negative statements about them"). On the other hand, the company may use a large damage request as another way to intimidate its critics into silence. DEMAC, *supra* note 22.

34. Furman, *supra* note 27, at 214 (noting that lawsuits are filed for the "primary purpose of uncovering an individual's identity"); Raney, *supra* note 25 (citing one anonymous defendant's lawyer who believes these lawsuits are a frivolous attempt to ascertain identities). For instance, the corporation may be looking to punish its own employees for violating privacy or other employment agreements. *See* Immunomedics, Inc. v. Doe, 775 A.2d 773, 777 (N.J. Super. Ct. App. Div. 2001) (holding that the corporation's right to subpoena the identity of an online speaker outweighed the speaker's right to anonymity where the evidence tended to prove that the speaker was an employee of the corporation in violation of certain company confidentiality agreements); Cook, *supra* note 28, at 30 (stating that proving an employee is violating policy would be easier to prove than libel).

35. Furman, *supra* note 27, at 218 (stating the purpose of filing the action is not to prove defamation but to silence the speech); Lidsky, *supra* note at 18, 881–82 (arguing that silencing John Doe is one of the largest motivations behind these corporate Internet defamation suits).

36. Civil Action No. 99-816 (Mass. Super. Ct., filed February 1, 1999).

37. Sobel, *supra* note 25, at ¶ 15.

consequences of such a suit.[38] Even if these new suits do not result in an award of damages, the "chill" can be felt when an online user is identified.[39] The Supreme Court has long recognized the importance of communicating anonymously as a part of the freedom of speech, stating that "anonymity is a shield from the tyranny of the majority."[40] Lower courts, following the Supreme Court's lead, thus apply strict scrutiny for any request to unmask anonymous defendants because of the potential for chilled speech.[41] The Court of Appeals for the Fourth Circuit, for instance, requires that a plaintiff demonstrate a compelling interest if the court foresees that a subpoena identifying an unknown speaker may chill the exercise of free speech.[42]

On the other hand, Professor Lyrissa Lidsky has argued that defamation suits may have a positive effect on Internet discourse as well.[43] Lidsky explains that these suits may help to "civilize cyberspace" in two ways. First, lawsuits will reduce the likelihood of defamation occurring in the first place.[44] Without fear of being attacked online, it is more likely that we will hear from all view points.[45] Second, allowing more defamation suits to proceed may help drive meaningless or abusive speech from message boards and chat rooms.[46] But not everyone agrees with Lidsky's theory, and the courts remain hesitant to remove the anonymity that the Internet provides for fear of generating a chill effect.[47]

3. Identifying the Proper Online Defendant

Finally, Internet defamation suits are unique because they become exceptionally complicated when trying to determine who the appropriate defendant should be. For instance, when an Internet user

38. Lidsky, *supra* note 18, at 888–89; *see also infra* notes 150–51 (discussing one award of three quarters of a million dollars to a company based on defamatory online remarks).

39. *See* Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117, 144 (1996) (arguing that forced revelation of a speaker's identity has serious and devastating effects on free speech discourse); Raney, *supra* note 25 (discussing the intent of company's filing suit against John Doe is only to seek his identity and chill such speech in the future).

40. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (invalidating an Ohio law that sought to prohibit anonymous pamphleting for political campaigns).

41. *See* Am. Constitutional Law Found. v. Meyer, 120 F.3d 1092, 1101–03 (10th Cir. 1997); Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

42. *See In re* Grand Jury Subpoena, 819 F.2d 1137 (Table) (4th Cir. 1987) (affirming the district court).

43. Lidsky, *supra* note 18, at 886–87.

44. *Id.*

45. *Id.*

46. *Id.*

47. *See supra* notes 38–41.

posts a statement to a chatroom, he may do so under a pseudonym; thus, the only information that a reader has about its author is the Internet site name and pseudonym.[48] Although it seems that traditional defamation law should hold Internet Service Providers[49] ("ISPs") liable for publishing defamatory material on their sites,[50] Congress has created a large safe haven for online publishers.[51] Originally, ISPs that exercised some editorial control over their postings could be held liable for defamatory statements that they published.[52] That rule changed, however, upon Congress's passage of the Communication Decency Act ("CDA").[53] A general trend among federal courts construing the CDA is for federal courts to refuse to hold ISPs liable for the postings on their sites, even when the ISPs consciously republish the material.[54] Thus, a defamed person or corporation's only option is to pursue legal action against the writer of such material.[55] But just who is this John Doe, and how does one sue him?

---

48. The ISP, however, may have more information about the user's identity. Most simply, an ISP is a company that provides access to the Internet to its customers. Jennifer Dolman, *When Can ISP's be Compelled to Identify Their Customers?*, THE LAWYERS WEEKLY, Vol. 22, No. 13 (Aug. 9, 2002), *available at* LEXIS, Nexis Library, The Lawyers Weekly News. When the user connects to the Internet through the ISP, the ISP assigns the user an Internet protocol, a numeric "address," which can be used to identify the anonymous online speaker. *Id.* Thus, an ISP has the means to trace a pseudonym back to a specific computer.

49. The Communications Decency Act defines "Internet Content Providers" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3).

50. *See infra* notes 201–02 and accompanying text.

51. 47 U.S.C. § 230(c) (2000) (mandating that no ISP should be treated as the author of any material provided by a user of its services).

52. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 23 Media L. Rep. 1794, 1799 (N.Y. Sup. Ct. 1995) (holding the Prodigy server liable for comments made by an online forum member libeling the Stratton Oakmont company because of the editorial control Prodigy maintained in deciding what material would be published online, thereby increasing its liability in defamation suits).

53. Communications Decency Act of 1996, Pub. L. No. 104-104 § 502(e), 110 Stat. 56, 133 (codified as amended in scattered sections of 18 and 47 U.S.C.).

54. Zeran v. Am. Online, Inc., 958 F. Supp. 1124, 1137 (E.D. Va.), *aff'd*, 129 F.3d 327, 335 (4th Cir. 1997) (holding that, under the CDA, an ISP is immune from liability for not removing defamatory material); Marczeski v. Law, 122 F. Supp. 2d 315, 327 (D. Conn. 2000) (holding the CDA shields this defendant from liability for the alleged defamation). Thus, AOL would not be liable for publishing defamatory content, but if a newspaper such as *The Washington Post* published such material, it might be liable. JEREMY HARRIS LIPSCHULTZ, FREE EXPRESSION IN THE AGE OF THE INTERNET 150 (2000) (citing Blumenthal v. Drudge, 992 F. Supp 44, 52–53 (D.D.C. 1998)).

55. Lidsky, *supra* note 18, at 872. It appears that the "Good Samaritan" sections of the CDA were intended to protect ISPs from liability only if they had, in good faith,

II. ONLINE DEFAMATION AND THE PROBLEMS OF SUING JOHN DOE

One major problem facing corporations as they try to hold someone legally accountable for defamatory online publication is that the author is anonymous. Most chat room users communicate under a pseudonym,[56] masking their true identity from others on the Internet.[57] The problem of suing an unknown defendant arose long before the Internet became popular, yet despite the increase in unknown parties, many of the difficulties with these suits continue.[58]

In several contexts, unknown defendants have been parties to legal action. For example, in property or estate settlement disputes, it is necessary to have all interested parties involved, but sometimes these parties are unknown.[59] In response, some states have drafted statutes permitting civil actions against unknown persons.[60] Other statutes address the issue of corporations operating under fictitious names,[61] allowing plaintiffs to sue the unknown owners or operators of such corporations.[62]

---

attempted to censor offensive material from their sites. *See* 47 U.S.C. § 230(c). Nevertheless, noticeably, the courts have created a much larger shield of liability.

56. George F. du Pont, Comment, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 191, 197–98 (2001). A pseudonym is a group of letters, symbols, and numbers that represent the online user.

57. There is, however, a distinction between true anonymity, which has a completely untraceable identity, and pseudo-anonymity, which can be traced through a series of difficult steps to discover the identity behind the pseudonym. *Id.* For purposes of this Comment, I consider both anonymous and pseudo-anonymous messages to be from unknown persons because the identity of the writer is unknown to the readers.

58. *See, e.g.*, Carol Rice, *Meet John Doe: It is Time for Federal Civil Procedure to Recognize John Doe Parties*, 57 U. PITT. L. REV. 883, 884 n.2 & 913–46 (1996) (discussing the inadequate rules of civil procedure for unknown parties in a lawsuit).

59. Chandler v. Ward, 58 N.E. 919, 924 (Ill. 1900) (defining necessary parties as those connected with the subject matter in question).

60. The statute in *Chandler*, for instance, provided that a suit involving an unknown party may proceed so long as the complaint acknowledges unknown parties, steps have been taken to find said parties, and notice has been given to these parties by publication. *Id.* at 925. If these steps are fulfilled, any court order will be binding upon the unknown defendants as if the suit were against their proper names. *Id.*

61. *See* CAL. CIV. PROC. CODE § 474 (West 1979) (indicating that a plaintiff may properly sue a corporation operating under a fictitious name so long as the plaintiff recites this in the pleadings and amends the complaint when the true name becomes known); *see also* Curtis v. Albion-Brown's Post, 219 N.E.2d 386, 388 (Ill. App. 1966) (citing an Illinois statute that requires all people conducting business under an assumed name to file, with the county clerk, a certificate identifying the owner, and allowing for suit against such owners).

62. *Curtis*, 219 N.E.2d at 389 ("Obviously the General Assembly intended that a cause of action arising out of the conduct or transaction of business be not defeated because of the claimant's inability to identify the individuals who in fact own and conduct the business.").

The Supreme Court first recognized a plaintiff's right to sue unknown defendants in *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*.[63] Webster Bivens sought relief for violation of his Fourth Amendment rights during his arrest by federal authorities.[64] Despite the fact that Bivens was unable to identify a single officer that had participated in his arrest, the district court ordered that his complaint be served on all "agents who it is indicated by the records of the United States Attorney participated in the arrest."[65] The Supreme Court upheld this order recognizing Bivens's right to seek relief on his infringed civil liberties from unknown defendants.[66]

Though some courts permit cases against John Doe defendants, it is often only under certain conditions. For instance, courts often require the plaintiff to describe the unknown defendant sufficiently to ensure that they are a legally accountable person or entity.[67] Next, the plaintiff may have to prove that the identity of the defendant is, in fact, unascertainable through the exercise of due diligence.[68] The standard of due diligence requires a good faith, honest effort on the part of the plaintiff to use reasonable effort (not all conceivable means) to discover the identity of the defendant.[69] Moreover, the plaintiff may have to prove that he is, in good faith, pursuing claims against the unknown parties in a timely manner,[70] and that he is not stalling to create new theories of liability. Finally, the plaintiff must attest, by affidavit, that he has met all of these requirements.[71]

---

63. 403 U.S. 388, 388 (1971).

64. *Id.*

65. *Id.* at 390 n.2.

66. *Id.* at 395–98.

67. *See* People v. Seda, 712 N.E.2d 682, 684 (N.Y. 1999) (holding the statute of limitations was tolled in a case where the state did not know the identity of the defendant, and referred to him merely as the "Zodiak killer").

68. Reed v. Gregory, 46 Miss. 740, 741–42 (1872) (explaining that, while the recently enacted state statute authorized notice by publication as a sufficient means of notice for unknown heirs in a chancery suit to divide the estate, such publication is only sufficient if the plaintiff first diligently attempts to ascertain the identity of the unknown, interested parties).

69. Berry v. Howard, 146 N.W. 577, 580 (S.D. 1914) (defining the standard of a due diligence search for unknown heirs).

70. Martin v. McCabe, 213 S.W.2d 497, 503 (Mo. 1948) (holding that if the defendant was unnamed merely due to a lack of reasonable inquiry by the defendant, judgment against the defendant is vitiated); *Berry*, 146 N.W. at 580 (holding that plaintiff did not exercise due diligence in discovering the identity of the unknown heirs and, therefore, notice to them by publication did not serve as reasonable notice).

71. *Berry*, 146 N.W. at 580.

Unknown defendant cases, however, raise several procedural problems and, as a result, some courts have refused to hear such cases.[72] These problems include the courts' jurisdiction over the defendant and the plaintiffs' amending the complaint to include the name of the defendant when it becomes known.

A. *Jurisdiction over John Doe*

1. Jurisdiction Generally

Before a court's order will be binding on a defendant, the court must ensure that it has both personal and subject matter jurisdiction.[73] First, the plaintiff must show that the court has personal jurisdiction over the defendant. Only in certain circumstances may a state court exercise personal jurisdiction over a non-resident defendant.[74] Since the plaintiff does not know the true identity or whereabouts of the defendant, it becomes technically impossible to meet this pleading requirement.[75]

The plaintiff must further demonstrate that the court has subject matter jurisdiction over the defendant. Subject matter jurisdiction will not present a problem if the company files in state court, however, as every state has a court of general subject matter jurisdiction.[76] But, lacking knowledge of an unknown defendant's residence could adversely affect the company's ability to file in

72. *See infra* notes 77–83 and accompanying text.

73. This is a two-part inquiry. First, the court must be authorized by statute to assert jurisdiction over the person, and second, the court's assertion of jurisdiction over the person must be constitutional under the Due Process Clause of the Constitution. *See generally* Pennoyer v. Neff, 95 U.S. 714 (1877) (discussing the personal jurisdiction requirement). The second part of this analysis is satisfied if the defendant has minimum contacts within the state trying to assert jurisdiction. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945). Moreover, the court may have general, personal jurisdiction, where it can hear any claim against the defendant, or specific jurisdiction, where it can only hear claims relating to the defendant's actions in the state.

74. These circumstances are discussed in the state's long arm statute. *See, e.g.*, N.Y. C.P.L.R. § 302 (McKinney 2001) (stating that a New York court can exercise jurisdiction over anyone who transacts business in the state, or commits a tort outside the state that harms anyone inside the state if he is engaged in regular business in the state or reasonably expects the consequences arising from this act to affect anyone in the state).

75. Rice, *supra* note 58, at 920 (noting that without knowing the identity of the person he is suing, a plaintiff cannot in good faith allege to know his citizenship).

76. *See generally* Morrell v. McCardle, No. C 98-0174 VRW (PR), 1998 U.S. Dist. LEXIS 1855, at *2 (N.D. Cal. Feb. 5, 1998) (stating that "[u]nlike state courts, they [federal courts] have no 'inherent' or 'general' subject matter jurisdiction").

federal court.[77] To determine whether subject matter jurisdiction exists, the Federal Rules of Civil Procedure require the plaintiff to set forth a "short and plain statement of the grounds upon which the court's jurisdiction depends."[78] If the plaintiff is entering federal court on diversity grounds, the plaintiff must prove that he and the defendant are citizens of different states.[79] When the defendant's whereabouts are unknown, a federal court cannot know whether it has diversity jurisdiction.

The courts' reactions to Doe defendants have been varied and unpredictable. One judge in the Northern District of Illinois, for instance, has refused to hear cases on diversity jurisdiction grounds when the defendant's identity is unknown.[80] While most other courts have not been so adamant in their refusal,[81] some have raised the bar for the plaintiff, requiring the plaintiff to attempt to prove Doe's citizenship before proceeding.[82] In 1987 the Ninth Circuit boldly refused to grant removal from state courts for any cases with a Doe defendant.[83] Congress acted quickly, however, passing a statute declaring that the citizenship of Doe defendants should be ignored for removal purposes.[84] Yet not all courts have concluded that this

77. *See supra* note 73 (discussing personal jurisdiction). These restrictions on jurisdictions, however, only limit a plaintiff's ability to file in federal court, with no effect on the state court option.

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

79. 28 U.S.C. § 1332(a) (2000).

80. *See* Salzstein v. Bekins Van Lines, Inc., 747 F. Supp. 1281, 1283 (N.D. Ill. 1990) (noting the court's disfavor of diversity jurisdiction in Doe defendant cases).

81. A district court in Hawaii, for instance, indicated that the plaintiff was assuming the risk by filing a diversity case in federal court when the citizenship of the defendant was unknown, and that court would dismiss the case if it later found that jurisdiction was improper. Macheras v. Center Art Galleries-Hawaii, Inc., 776 F. Supp. 1436, 1440 (D. Haw. 1991) ("A plaintiff who names Doe defendants, files suit in federal court at his peril."); *see also* Weber v. Kosack, 96 Civ. 9581 (LMM), 1997 U.S. Dist. LEXIS 16786 at *7–9 (S.D.N.Y. Oct. 24, 1997) (discussing the struggle that federal courts face in determining whether unknown parties meet the requirement of diversity jurisdiction and denying defendant's motion to dismiss the case for lack of subject matter jurisdiction).

82. *See* Dunn v. Paducah Int'l Raceway, 599 F. Supp 612, 613 n.1 (W.D. Ky. 1984) (determining that a Doe defendant does not destroy good faith allegations of diversity of citizenship).

83. Bryant v. Ford Motor Co., 844 F.2d 602, 605 (9th Cir. 1987) (citing frustration with the lack of consistency in the federal circuits, the court, sitting en banc, created an outright ban on state claims with Doe defendants).

84. Judicial Improvements and Access to Justice Act, Pub. L. No. 100-702, § 1016(a), 102 Stat. 4642, 4669 (1988) (codified at 28 U.S.C. § 1441(n) (2000)). Commentary to the rule suggests that if the identity of the defendant is later found to destroy diversity, the court should act (under 28 U.S.C. § 1447(e) (2000)) to either deny joinder or permit joinder and remand the case back to the appropriate state court. H.R. REP. NO. 100-889, at 71 (1988), *reprinted in* 1988 U.S.C.C.A.N. 6031, 6031–32.

statute applies to the original complaint,[85] and there remains no clarity on diversity jurisdiction over Doe defendants.[86]

2. Jurisdiction and the Internet

Suits arising over Internet activity add a new dimension to the jurisdiction question. To determine whether a state may constitutionally assert jurisdiction over a defendant, the defendant must meet the "minimum contacts" test,[87] meaning that he must "purposefully avail" himself of contacts within the forum state.[88] A plaintiff could argue, then, that any defendant who commits a crime or tort on the Internet meets this standard in every state in the country because Web sites are accessible everywhere there is an Internet connection. There is no easy way to allow residents of only one state to access a Web site.[89] Courts, therefore, have not found that such a broad reading of the minimum contacts requirement is appropriate for all actions involving the Internet.[90]

The judicial trend is a "sliding scale" for the evaluation of the defendant's contacts. This approach requires the court to analyze the scope and breadth of the Internet contacts. Under this approach, the court considers both the quality and quantity of the entity's online activity to determine if it may constitutionally exercise personal jurisdiction.[91] The more significant and commercial the activity, the more likely that jurisdiction is proper. Thus, a defendant who knowingly enters into repeated online contracts with residents of a state can expect that the state may properly assert jurisdiction over

85. *See Salzstein*, 747 F. Supp. at 1283.

86. Rice *supra* note 58, at 925 (stating that "the question of a Doe defendant's impact on diversity jurisdiction may be even more confused today").

87. *See* Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (citing Pennoyer v. Neff, 95 U.S. 714, 733 (1877)).

88. Hanson v. Denckla, 357 U.S. 235, 253 (1958) (holding that to meet minimum contacts, the defendant must do some act to purposefully avail himself of the privilege of conducting business in the state).

89. For instance, a company could limit access to its Web site to residents of a single state by mailing each resident of the particular states a user-name and password to access the site, but, doing so would add substantial costs, making this suggestion unrealistic.

90. In *Weber v. Jolly Hotels*, 977 F. Supp. 327 (D.N.J. 1997), for instance, a New Jersey district court stated that the mere presence on the Internet will not satisfy the minimum contacts requirement needed for the court to exercise personal jurisdiction over the non-resident defendant. *Id.* at 333. *But see* Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 164–65 (D. Conn. 1996) (applying a broad view of Internet contacts and holding the defendant liable when residents of the forum state did access the Web site).

91. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

him.[92] On the other hand, under this approach, the operator of a "passive"[93] web site will not be subject to jurisdiction in every state.[94]

This approach will provide little help for plaintiffs wishing to sue unknown defendants for defamatory comments posted on Internet Web sites. Courts will likely place defendants that merely post messages online, rather than operating a Web site or running an online business, at the lowest end of the spectrum. By merely placing a comment in a medium publicly available throughout the world, the defendant's conduct would not satisfy the minimum contacts test and, unless the defendant had another, stronger connection to the forum state, asserting personal jurisdiction over the defendant in such a case would not be constitutional.[95]

B. Statute of Limitations Bar and the Relation Back Doctrine

Claims of online defamation, like virtually every legal action, are subject to statutes of limitations that, after a certain amount of time, will bar the plaintiff from pursuing her claim.[96] Most courts recognize that the purpose of pleading against a John Doe defendant is to file one's claim before the statute of limitations runs out even though the true identity of the defendant is not yet known.[97] As one court asked, "Should a plaintiff lose his right to have his case tried because of ignorance of the names of parties whom he has a right to sue, and as to whom he may have a good cause of action?"[98] The Federal Rules

92. *E.g.*, Compuserve, Inc. v. Patterson, 89 F.3d 1257, 1263 (6th Cir. 1996) (holding a defendant who marketed his product through a local service provider had purposefully availed himself of doing business in that state and personal jurisdiction over him was properly asserted).

93. A passive site is one that does no more than provide information; the site and the viewer do not interact beyond the displaying of static information. *See Zippo Mfg.*, 952 F. Supp. at 1124.

94. Bensusan Rest. Corp. v. King, 937 F. Supp. 295, 299 (S.D.N.Y. 1996) (holding that the defendant did not purposefully target residents of the forum state and, therefore, jurisdiction was not proper based on his online activity).

95. *Weber*, 977 F. Supp.at 333 (holding that the defendant did not attempt to conduct business by placing pictures of its hotel rooms over the Internet and that, as a "passive" site, personal jurisdiction over the Italian company was not proper).

96. Faigan v. Doubleday Dell Publ'g Group, Inc., 98 F.3d 268, 271–72 (D. Wis. 1996) (discussing how the state's borrowing statute—which states that, for a "foreign" claim where the injury occurred outside of the home state, the proper statute of limitations will be the shorter between the home and foreign state—will be difficult to implement for Internet defamation cases).

97. *E.g.*, Craig v. United States, 413 F.2d 854, 856 (9th Cir. 1969) ("The only purpose the naming of fictitious defendants could possibly serve is to make it possible to substitute named defendants after the statute of limitations has run.").

98. Larson v. Barnett, 225 P.2d 297, 302 (Cal. 1950) (quoting Irving v. Carpentier, 11 P. 391, 392 (Cal. 1886)) (discussing a provision in the state's civil procedural rules that

of Civil Procedure seemed to have answered this question when it created the "relation back doctrine;" upon closer consideration, however, it appears that the new rules may generate more problems for these plaintiffs than they solve.[99]

To correct mistakes in the original pleadings, the relation back doctrine permits a plaintiff to amend its pleadings, in certain defined circumstances, after the statute of limitations has run on a claim.[100] A plaintiff seeking to amend another party's name in the complaint after the statute of limitations has run must meet the three-part test contained in Rule 15(c)(3): (1) the claim in the amended pleading arises from the same transaction as the original pleading; (2) the new party had timely notice of the lawsuit; and (3) the new party "knew or should have known that, but for a mistake concerning the identity of the proper party, the action would have been brought against the party."[101]

An illustration is most helpful to understand the problems created by the relation back doctrine. Assume Company XYZ notices a decline in its stock price over a year. Looking for answers, company officials scour the Internet and find defamatory remarks about the company on a certain Web site devoted to the company. The XYZ officials believe these remarks are the reason for their damaged stock value and they want to sue the writer for defamation. The writer is operating under the pseudonym "Bad-Boy," and the corporation has no way of ascertaining his real identity. The statute of limitations on defamation is one year[102] so XYZ corporation files suit against the unknown Bad-Boy to save its claim from being barred.[103] Subsequently, during the course of discovery, Bad-Boy's identity is revealed and XYZ wants to amend its complaint to state his name. In order to amend the complaint, XYZ must satisfy the three-part standard of Rule 15(c)(3). Upon a literal reading of these

---

enables a plaintiff to file suit against a fictitious party when the defendant's true identity is unknown).

99. Rice, *supra* note 58, at 927 (noting the irony in that the relation back doctrine, which was created to deal with Doe defendants, now creates the largest problems for them).

100. *See* Dore v. City of Fairbanks, 31 P.3d 788, 791 (Ala. 2001).

101. FED. R. CIV. P. 15(c)(3)(B).

102. N.C. GEN. STAT. § 1-54(3) (2001). Again, defamation is a state law action, so the statute of limitations may vary from state to state.

103. Other statute of limitations issues may arise here such as when the cause of action actually accrued. These problems are beyond the scope of this Comment.

requirements, however, XYZ, or any similarly-situated plaintiff, would be unable to meet the test of Rule 15(c)(3).[104]

The first requirement of the relation back test—requiring that the claim in the amended complaint arise from the original complaint—should always be met when the plaintiff is seeking to amend to substitute the name of a defendant.[105] In this hypothetical, the amended complaint would recite the same facts and cause of action. The second relation back requirement should be satisfied if the plaintiff moves to amend the complaint and serves the new defendant within 120 days[106] of filing the original complaint. At least one court has found that serving the identified defendants unequivocally operates as adequate notice to the Doe defendants.[107] Even if discovery is not started immediately, a diligent XYZ should be able to get this necessary information and move to amend its complaint within the prescribed time frame.

The third requirement in Rule 15(c) discusses permission to amend the complaint when the plaintiff was mistaken about the identity of the defendant. In most Doe defendant cases, the plaintiff is not mistaken about the identity of the party, the plaintiff corporation just does not know it. The question, therefore, is whether this amounts to a "mistake in identity" under the relation back doctrine? The federal courts that have explored this issue have come up with three different approaches to answering this question.[108]

The first approach applies a literal meaning to mistake and forbids amending the complaint under Rule 15(c)(3) if it is to add the identity of a defendant who was originally unknown.[109] In *Wood v. Worachеck*,[110] the Court of Appeals for the Seventh Circuit was the first to implement this approach, holding that a lack of knowledge of

104. Rice, *supra* note 58, at 927–31.

105. *Id.* at 928 (noting that the amended pleading in these cases is generally a verbatim recitation of the first complaint, differing only in the substituted name).

106. This number comes from a careful reading of the rule, requiring these steps to be taken within the period expressed in Rule 4(m) of the Federal Rules of Civil Procedure. FED. R. CIV. P. 4(m).

107. Cruz v. City of Wilmington, 814 F. Supp. 405, 410 (D. Del. 1993). Not giving the newly-identified party notice within this time frame may, on the other hand, eliminate the opportunity to amend the complaint. *See, e.g.*, Craig v. United States, 413 F.2d 854, 857–58 (6th Cir. 1969) (holding the motion to amend did not relate back due to untimely notice).

108. *See* Steven S. Sparling, Note, *Relation Back of "John Doe" Complaints in Federal Court: What You Don't Know Can Hurt You*, 19 CARDOZO L. REV. 1235, 1253–74 (1997).

109. Rice, *supra* note 58, at 930–32 (noting that such a literal reading of the rule does not comport with its purpose, which is to increase flexibility in amending complaints).

110. 618 F.2d 1225 (7th Cir. 1980).

a party's identity is not an error as necessitated under the rule, and, therefore, it did not matter whether the substituted defendant should have known of the suit.[111] Under the second approach, courts interpret the relation back rule very broadly as it applies to Doe defendants. These courts have held that "mistake" should include any circumstance of improperly naming the defendant,[112] thereby including the situation in which the original defendant is unknown. Under this second approach, a plaintiff should be allowed to amend a complaint to add the previously unknown identity of the defendant. Finally, the third approach ignores the word "mistake," focusing on a factual determination of whether the amended defendant had adequate notice. Although no appellate court has adopted this approach as the test under Rule 15(c)(3), at least one legal commentator claims that focusing on notice is the best approach.[113]

Thus, amid the confusion surrounding the meaning of mistake under the relation back doctrine, the plaintiff may be barred from amending a complaint based on a lack of knowledge of the identity of the defendant. This seems an inherently unfair hurdle and one that needs to be clarified through either a Supreme Court decision or a substantive change in the Federal Rules of Civil Procedure.

III. THE INTERNET DEFAMATION CASES AGAINST JOHN DOE

Because there are so many problems with suing unknown defendants, it is unclear what steps potential plaintiffs should take. Usually, once the suit is filed, the first step for judicial interference occurs when the corporation files a subpoena on the anonymous defendant's ISP, requesting identifying information about the speaker.[114] In California, for instance, the plaintiff will have to make

111. *Id.* at 1230 (holding the plaintiff could not properly amend his complaint once several defendant police officers had been identified, stating that Rule 15 "does not permit relation back where, as here, there is a lack of knowledge of the proper party").

112. Rice, *supra* note 58, at 930, 933–35 ("A mistake within the meaning of the rule exists whenever a party who may be liable for the actionable conduct alleged in the Complaint was omitted as a party defendant." (citing Williams v. Avis Transport of Canada, 57 F.R.D. 53, 55 (D. Nev. 1972))).

113. *Id.* at 930, 937–39 (calling this the "best approach" because it captures the goal of the relation back doctrine and is fair to all parties). Rice does note that one district court has used this approach. *See* Campbell v. Berferon, 486 F. Supp. 1246, 1251 (M.D. La. 1980), *aff'd*, 654 F.2d 719 (5th Cir. 1981).

114. Many ISPs receive requests for user identities. *See* Jeffrey Terraciano, *Can John Doe Stay Anonymous?*, WIRED.COM, Feb. 21, 2001, *at* http://www.wired.com/news/privacy/0,1848,41714,00.html (on file with the North Carolina Law Review). America Online reported handling nearly five hundred subpoena requests in the year 2000 alone. *See* Jeffery Brenner, *Chat Room Rants Protected*, WIRED.COM, Feb. 27, 2001, *at* http://

such a request ex parte because the state Code of Civil Procedure requires a showing of good faith before discovery can take place in a suit in which the defendant has not been properly served.[115] Usually, the ISP will then notify the defendant that his personal information is being sought,[116] and the potential defendant will be responsible for fighting the subpoena. Because many Internet defamation cases are dropped upon identification of the anonymous speakers,[117] this Comment only examines the motions for subpoenas by the allegedly defamed companies. There have been very few of these cases based on motions to quash such subpoenas, and although no definite standard has emerged with which to analyze these requests, it is clear that the burden on the corporation seeking the identifying information will be very high.[118]

The first important case, *Columbia Insurance Co. v. Seescandy.com*,[119] involved a suit for trademark infringement.[120] The plaintiff sought a temporary restraining order but did not know the

---

www.wired.com/news/politics/0,1283,42039,00.html (on file with the North Carolina Law Review). Roger Rosen and Charles Rosenberg, two attorneys who practice in this area regularly, advise their clients to serve very broad subpoenas on the ISP asking for all information the ISP may have of the user's account—name, address, email address, telephone numbers, as well as a log of the postings by the anonymous poster. Roger Rosen & Charles Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, THE COMPUTER & INTERNET LAW., Feb. 2002, at 9. This could be a double-edged sword, however, since at least one court considered a broad subpoena request an instance of bad faith. Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088, 1096 (W.D. Wash. 2001).

115. CAL. CIV. PROC. CODE. § 2025(b)(2) (West 1979).

116. How an ISP deals with a request for an identity may depend on its particular privacy policy. Yahoo!'s policy, for instance, explains to users that their identifiable information may be disclosed in response to subpoenas, court orders or legal process. YAHOO! PRIVACY, INFORMATION SHARING AND DISCLOSURE, *at* http://privacy.yahoo.com/privacy/us/sbc/details.html (last visited Oct. 28, 2002) (on file with the North Carolina Law Review). Similarly, Microsoft Network discloses user information to "conform to the edicts of the law or comply with legal process served on Microsoft or the site." MSN, MSN STATEMENT OF PRIVACY, *at* http://privacy.msn.com (last visited Oct. 28, 2002) (on file with the North Carolina Law Review). Neither ISP promises notification before complying with such a legal request, but it is the policy of each to do so. Terraciano, *supra* note 114 (quoting Nicole Berner, an attorney with Jenner and Block, familiar with Yahoo!'s policies).

117. Raney, *supra* note 25 (discussing the Raytheon case that was dropped upon revelation of the identities of twenty-one online critics); Terraciano, *supra* note 114 (noting another company that dropped its suit once the defamatory messages stopped appearing on the website).

118. *E.g.*, *2themart.com*, 140 F. Supp. 2d at 1097 (arguing that courts should impose a high threshold on corporations seeking information identifying online users).

119. 185 F.R.D. 573 (N.D. Cal. 1999).

120. *Id.* at 575.

true identity or location of all of the defendants.[121] The court explained that because of problems with lack of proper service and jurisdiction, John Doe cases are typically discouraged; however, the Internet has created new opportunities for tortious activity by anonymous or pseudonymous actors, and the plaintiffs in these cases should not be left without relief.[122] Thus, the court created a four-factor test to determine when a plaintiff, acting in good faith, has a legitimate claim that deserves court intervention.[123]

First, the plaintiff must identify the unknown defendant with enough specificity to prove to the court that the defendant is a person that can be sued in federal court.[124] Second, the plaintiff must make a good faith attempt to comply with service requirements and locate the unknown party.[125] In *Columbia Insurance Co.*, the plaintiffs attempted to satisfy this requirement by delivering service papers to all known email addresses of the defendant.[126] The court held that while this was not proper service, it did represent a good faith effort to comply with these rules.[127] Next, the plaintiff must prove that the action would survive a motion to dismiss. The purpose of this requirement is to ensure that the plaintiff has filed a legitimate suit and is not filing the case to intimidate or harass the potential defendants.[128] Finally, the plaintiff must file a discovery request with a list of the information sought, indicating how the plaintiff will use this information to cure the existing defects with service of the underlying suit.[129] The court thus gave the plaintiff fourteen days to comply with this fourth requirement.[130]

Other courts that have dealt with the issue of corporations seeking the identity of unknown online defamers have created similar tests. The only appellate court that has addressed this issue is the Appellate Division of the Superior Court of New Jersey.[131] In two

121. *Id.* at 578–79. The plaintiff named some of the defendants by their online pseudonyms, some by their site post names, and others by the registered identity.

122. *Id.* at 578.

123. *Id.* at 577–78.

124. *Id.* at 578. A court always has jurisdiction to determine whether or not it has personal jurisdiction over a suit. Wells Fargo & Co. v. Wells Fargo Express Co., 556 F.2d 406, 430 (9th Cir. 1977).

125. *Columbia Ins. Co.*, 185 F.R.D. at 579.

126. *Id.*

127. *Id.*

128. *Id.* at 579–80.

129. *Id.* at 580.

130. *Id.*

131. *See* Dendrite Int'l, Inc. v. Doe, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001); Immunomedics, Inc. v. Doe, 775 A.2d 773, 777 (N.J. Super. Ct. App. Div. 2001).

cases decided on the same day, the court created a very high, but not insurmountable standard for the plaintiff to succeed with a subpoena on the ISP.[132]

In the first case, *Dendrite International, Inc. v. John Doe*,[133] the plaintiff was a corporation claiming that the defendants (John Does numbered 1–14) had defamed the corporation on the ISP's bulletin board. As a result, the corporation sought discovery of identifying information from the ISP.[134] By balancing the defendant's First Amendment rights against the plaintiff's right to protect its reputation, the court created a three-part test the plaintiff must satisfy to compel an ISP to reveal the online users' identities.[135] First, the plaintiff must prove that she has made a good faith attempt to notify the defendants that they are the subjects of the subpoena, giving the defendant reasonable time to respond to such a request.[136] Second, the court should require the plaintiff to identify the specific statements made by the defendants.[137] Third, the plaintiff must set forth a prima facie case for a defamation action.[138] Although the court cited *Columbia Insurance Co.* in creating the third prong, the New Jersey court seemed to be imposing a much higher showing than the *Columbia Insurance Co.* court required in the trademark infringement case.[139]

Here, the appellate court acknowledged that Dendrite had proved the three basic elements of a defamation cause of action: (1) identifying the defamatory statements; (2) identifying the utterer; and (3) establishing that the statements were published.[140] The court agreed with the trial judge, however, that the plaintiff had failed to prove harm from the defamatory statements, and thus had not met its

132. *See infra* notes 135–39 and accompanying text.
133. 775 A.2d 756 (N.J. Super. Ct. App. 2001).
134. *Id.* at 756–57.
135. *Id.* at 760–61.
136. *Id.* at 760.
137. *Id.*
138. *Id.*
139. The court in *Columbia Insurance Co. v. Seescandy.com* required only that the plaintiff bring a legitimate claim in good faith. 185 F.R.D. 573, 578 (N.D. Cal. 1999). In *Dendrite*, however, the court demanded that the plaintiff prove that it had a prima facie case. *Dendrite*, 775 A.2d at 760.
140. Based on establishing these elements, Dendrite continued to plead that it had met the prima facie requirement that the *Seescandy.com* court had created. *Dendrite*, 775 A.2d at 768–70 (citing Zoneraich v. Overlook Hosp., 514 A.2d 53, 63 (N.J. Super. Ct. App. Div. 1986)).

burden.[141] The trial court analogized the subpoena request to a motion by the government to seek discovery, and noted that a heavy burden on the plaintiff was necessary to ensure that the discovery process was not being abused.[142] Nonetheless, the appellate court affirmed the denial of the subpoena request because Dendrite failed to prove that it had been harmed by the defamatory statements.[143] This ruling raises the question of why the plaintiff would need to prove harm in the earliest of discovery motions, before the defendant had even been identified and when harm was not an element of its claim.

In the other case decided by the New Jersey Superior Court Appellate Division on the same day, the court denied a defendant's motion to quash the subpoena served on an ISP to identify an anonymous defendant.[144] In *Immunomedics, Inc. v. Doe*,[145] the plaintiff claimed the defendant was an employee of Immunomedics that had breached a confidentiality agreement based on its online comments.[146] The court found that the corporation's right to learn the defendant's identity outweighed the user's right to remain anonymous because Immunomedics clearly had established a prima facie cause of action.[147] Unlike *Dendrite*, the court did not require Immunomedics to prove that the defendant's conduct had caused it harm, nor did the court attempt to distinguish why the *Dendrite* case had required this showing.

At about the same time the New Jersey appellate courts were ruling, a Virginia trial court was reviewing a subpoena order from an Indiana court on America Online ("AOL"), a Virginia corporation. The Indiana court had ordered AOL to reveal the identities of five anonymous online critics of an Indiana company that also sought to remain anonymous, citing potential economic harm if it revealed its identity before it knew the identity of the defendants.[148] The Virginia trial court created yet another standard, holding that the subpoena

141. *Id.* at 770. The court said that it refused to "take the leap" that the posting of the negative messages had some connection to a decline in stock price of Dendrite without something more concrete to go on. *Id.* at 769–70.

142. *Id.* at 770–71.

143. *Id.* at 772.

144. Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. Super. Ct. App. Div. 2001).

145. *Id.*

146. *Id.* at 776.

147. *Id.* at 777–78.

148. In re Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372, at *1 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds*, Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

should be enforced if the plaintiff first provides a good faith basis for the belief that it is the victim of actionable conduct by the defendants and second, that the information sought is crucial to advancing the plaintiff's claim.[149] The Supreme Court of Virginia later reversed this decision, not based on the subpoena standard, however, but because the Indiana court improperly ruled that the online speaker could remain anonymous.[150] Again, the appellate court missed an opportunity to clarify the standard on subpoena motions.

A federal district court in Washington recently addressed this issue and created yet another, similar test for balancing the First Amendment rights of the online users to remain anonymous versus the right of a plaintiff to seek discovery for a claim or defense. In *John Doe v. 2themart.com*,[151] the court quashed a subpoena of an ISP because the plaintiff failed to prove that the subpoena was directly and materially related to its lawsuit.[152] 2themart.com was facing a derivative lawsuit by its shareholders and was seeking the identity of twenty-three online speakers who had posted defamatory comments about the corporation, and sought to prove through the subpoenaed evidence that its stock price was declining not due to its own actions but due to the illegal activities of the unknown critics.[153] The court missed the connection and said it was unclear what effect these defendants would have on the underlying derivative suit.[154] The court adopted the following four-factor test for evaluating a subpoena to identify a non-party to the lawsuit. First, the subpoena must be in good faith, and not for an improper purpose such as to harass or intimidate.[155] Second, the information sought must relate to the underlying claim.[156] Third, the information must be "directly and materially relevant" to the underlying claim or defense.[157] Finally, the

149. *Id.* at *8.

150. Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 385 (Va. 2001).

151. 140 F. Supp. 2d 1088 (W.D. Wa. 2001).

152. *Id.* at 1097–98.

153. *Id.* at 1091–97.

154. *Id.* at 1097.

155. *Id.* at 1095. The court held that the huge scope of the original subpoena tends to show a lack of good faith on the part of 2themart.com. *Id.* at 1096.

156. *Id.* at 1095–96. In analyzing this factor under the current facts, the court held that if the information sought related only to one of numerous claims or defenses, then it was not worth compromising the party's First Amendment right to anonymity. *Id.* at 1096. Here, the information would prove one of 2themart.com's twenty-seven affirmative defenses. *Id.*

157. *Id.* at 1095.

information sought must be unavailable from another source.[158] Based on the facts before it, the court concluded that many of these factors weighed in favor of quashing the subpoena motion.[159] Though this case was unique because the plaintiff sought the identity of non-parties to the suit and not the identity of the defendants, the case illustrates yet another approach employed by a misguided court to balance the First Amendment right of the anonymous online speaker with the interests of the corporation in uncovering the identity of the speaker who allegedly defamed the corporate reputation.

While at least one trial court has found sense enough amid this confusion to follow a precedent,[160] the majority of recent cases confirm that the lower courts lack a consistent rule to follow when considering subpoenas for the identity of alleged online defamers. For instance, one California federal district court recently dismissed a corporation's defamation action against anonymous Internet posters.[161] District Judge David Carter held that the Internet postings were not defamatory, under California law, because they represented statements of opinion rather than fact.[162] A year earlier, however, another federal district court in California took a much different approach to a corporate Internet defamation lawsuit. In *Felch v. Day*,[163] Varian Medical Systems was awarded a $775,000 jury verdict against former employees based on nearly fourteen thousand defamatory messages spanning one hundred different Internet Web sites.[164] In addition, the judge ordered a permanent injunction against

158. *Id.* The court found that 2themart.com had not met this factor because some of the information that they sought was archived by the ISP and was available to the public. *Id.* at 1095–97.

159. *Id.*

160. Applying the four-factor *Dendrite* test, the New Jersey trial court ruled in favor of quashing a subpoena requested by the Town Council to identify online, libelous critics. The judge ruled that the Council failed to plead with sufficient specificity and also failed to adequately notify the potential defendants, therefore, not meeting two of the factors articulated by the New Jersey appellate court. Mary P. Gallagher, *Defamation Plaintiffs Cannot Learn Anonymous Online Critics' Identities*, 167 N.J. L.J. 4, 4, 15 (2002).

161. Global Telemedia Int'l v. Doe, 132 F. Supp. 2d 1261, 1271 (C.D. Cal. 2001).

162. *Id.* This ruling has pleased several Internet privacy experts who have long been arguing that online message board postings should be analyzed under the opinion exception to defamation. Brenner, *supra* note 114; *see also supra* text accompanying notes 16–18 (discussing the opinion exception).

163. 238 F.3d 428 (Table), 2000 WL 1364444 (9th Cir. 2000) (vacating a preliminary injunction issued by the United States District Court for the Northern District of California). Upon remand, the jury awarded the plaintiff $775,000. Stephanie Armour, *Courts Frown on Online Bad-Mouthing*, USA TODAY, Jan. 7, 2002, at 1B.

164. *Id.* at 428; Armour, *supra* note 163. The allegedly defamatory messages included complaints of discrimination by company personnel against gays and pregnant women. *See* Armour, *supra* 163.

the message writers.[165] The Court of Appeals for the Third Circuit, similarly rejected defendants' First Amendment defense, but the court did not issue an oral or written opinion, leaving the constitutional questions unsettled.[166]

The only thing that remains clear after analyzing these cases is that there is no definite, uniform standard for a corporation seeking the identity of an unknown defendant for defamation on the Internet. All parties involved—plaintiffs, defendants, and legal commentators—agree that the increasing number of online defamation cases combined with the fundamental right of free speech amplify the need for tighter judicial scrutiny and a well-established doctrine in this area.[167] Until such a doctrine exists, a plaintiff seeking the identity of unknown, alleged defamers should be prepared for any one of several standards that it may have to meet. From a minimal showing that without the identifying information the plaintiff is unable to properly serve the correct defendant, to an extensive showing that his claim can survive a motion for summary judgment, plaintiffs in these Internet defamation suits face a severe disadvantage of not knowing their burden.[168]

IV. A POTENTIAL SOLUTION: USE OF THE SIMILAR, SETTLED JURISPRUDENCE OF THE JOURNALIST'S PRIVILEGE

ISPs are similar to reporters in many ways. First, both facilitate the dissemination of information to the public, and both gather and

165. Order Granting Plaintiff's Motion for Preliminary injunction, June 21, 1999, *at* http://www.geocities.com/mobeta_inc/slapp/whyteorder.html (on file with the North Carolina Law Review).

166. Collins, *supra* note 3 (exploring a recent Third Circuit decision to not publish its opinion on this subject).

167. Memorandum In Support of Motion of J. Doe to Quash Subpoena Issued to Silicon Investor/Infospace, Inc., Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001) (No. C01-453Z) (asking the court, in an amicus curiae brief filed by the American Civil Liberties Union, to clarify the standard upon which disclosure of an anonymous posters identity can be revealed); Terraciano, *supra* note 114 (discussing the disappointment of the defendant in an online defamation case after settling because he wanted to go to trial to set precedent that corporations cannot get private information just for alleging that they were wronged). David Sobel, the general counsel for the Electronic Privacy Information Center, has often been quoted as wanting the courts to set a legal standard that would protect the First Amendment rights of online posters. *See, e.g.*, Brenner, *supra* note 114 (discussing how an ISP deals with requests for identity); Raney, *supra* note 25 (discussing the appeal of Internet anonymity).

168. Rosen & Rosenberg, *supra* note 114, at 9 (citing Bernson v. Browning-Ferris Indus., Inc., 873 P.2d 613, 624 (Cal. 1994) (Kennard, J., dissenting)); *see* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577–81 (N.D. Cal. 1999); Dendrite Int'l., Inc. v. Doe, 775 A.2d 756, 767–72 (N.J. Super. Ct. App. Div. 2001).

distribute this information in the course of their normal activity, not in preparation for lawsuits.[169] Second, both could suffer devastating effects if they lose the trust of their information providers. As a reporter argued in *Branzburg v. Hayes*,[170] trust is an essential element for reporters in maintaining informants;[171] likewise, computer users also seek privacy in their on-line dealings.[172] Many commentators, in fact, have argued that Internet speech would face a severe chill, as users would be more reluctant to speak out on the Internet if they worried that their identities could be revealed.[173] Fearing a lack of anonymity, people may not want to speak to reporters or to post comments on Internet message boards, thereby resulting in a loss of a large pool of potential information.

Journalists have long used the Federal Rules of Civil Procedure to quash subpoena motions[174] and have further asserted a journalist's privilege to avoid divulging information to trial courts and grand juries in both criminal and civil cases. The policy interests advanced in these journalist cases are so similar to that of Internet defamation suits that the test consistently applied by courts in journalist cases is an adequate guide for analyzing the subpoenas on ISPs. Thus, this comparison would give plaintiffs in Internet defamation suits an established burden to meet when seeking identifying information from ISPs. The following discusses the case law involving subpoenas served on reporters to reveal an anonymous source.

---

169. Memorandum In Support of Motion of J. Doe to Quash Subpoena Issued to Silicon Investor/Infospace, Inc., Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wa. 2001) (No. C01-453Z).

170. 408 U.S. 665 (1972).

171. *Id.* at 671 n.6.

172. At least one Internet user has fought back, suing an ISP that provided a company with his identifying information. Writing under the name "Aquacool_2000," the user made derogatory remarks about AnswerThink, a consulting company. When AnswerThink sued in federal court in California, Yahoo! quickly revealed Aquacool_2000's identity. Aquacool_2000 then sued Yahoo!, alleging a breach of privacy, but the two parties settled, so a court did not rule on the legitimacy of the claims. Dan Bischof, *Through Accusations of Defamation, Companies are Starting to Unmask Anonymous Online Critics*, NEWS MEDIA & THE LAW, Winter 2001, at 35, http://www.rcfp.org/news/mag/v.cgi?25-1/lib-anonymou (on file with the North Carolina Law Review); *see also* Cohen v. Cowles Media Co., 501 U.S. 663, 671–72 (1991) (holding that the First Amendment is not a defense for a claim of promissory estoppel where a reporter breached a promise of confidentiality to an informant).

173. *See supra* notes 38–42 and accompanying text.

174. The rules provide that a court shall quash or otherwise modify a subpoena if it requires disclosure of protected matter, and courts may do the same if the subpoena requires disclosure of confidential research, in order to protect the person affected by the subpoena. FED. R. CIV. P. 45(c)(3)(A)&(B).

In the landmark decision of *Branzburg v. Hayes*,[175] the Supreme Court rejected a reporter's assertion of journalistic privilege when he was ordered to testify in front of a grand jury.[176] In that case, the reporter had written a published piece on the marijuana trade and had used anonymous sources in his story.[177] The piece implicated unknown sources in criminal activity, and the Court held the reporter did not have a constitutional right to conceal relevant facts of the case when the grand jury investigated the crimes.[178] The Court recognized the result may have some "chill" effect on news reporting, as some informants may not wish to be interviewed for fear of later criminal proceedings. This effect, however, was outweighed by the "public interest in pursuing and prosecuting those crimes reported to the press."[179] Although the opinion of the Court rejected this assertion of privilege, a majority of the justices recognized that reporters do have a qualified First Amendment privilege.[180]

Branzburg also stands for the proposition that subpoenas seeking a journalist's information need to be considered on a case-by-case basis.[181] Courts have thus assiduously analyzed journalists' privilege claims, recognizing the important policies competing in these cases. On one hand, the right to seek relief in a court of law is paramount in a civilized society,[182] and prolific discovery is an essential part of our judicial system, as shown in both substantive[183] and procedural[184] rules alike. On the other hand, our society values the free flow of ideas, and imperative to that flow is the ability of news reporters to collect, assemble, and distribute information to the public.[185] Thus, the

175. 408 U.S. 665 (1972).

176. *Id* at 708–09. The journalistic privilege, a privilege created by state law, exempts professional journalists from testifying in court based on information they received while reporting on or gathering the news. *E.g.*, FLA. STAT. ANN. § 90.5015(2) (West 1999) (discussing the journalistic privilege).

177. *Branzenburg*, 408 U.S. at 667–68 (noting that the article stated that the reporter had promised the subjects that their identities would not be revealed).

178. *Id.*

179. *Id.*

180. This was observed by Judge Merhige in *Gilbert v. Allied Chemical Corp.*, 411 F. Supp. 505, 509 (E.D. Va. 1976).

181. *Branzburg*, 408 U.S. at 709–10 (Powell, J., concurring).

182. Garland v. Torre, 259 F.2d 545, 549 (2d Cir. 1958).

183. "The law begins with the presumption that the public is entitled to every person's evidence." Richards of Rockford, Inc., v. Pac. Gas & Elec. Co., 71 F.R.D. 388, 389 (N.D. Cal. 1976) (citing Blackmer v. United States, 284 U.S. 421 (1932)).

184. *See* FED. R. CIV. P. 26(b)(1) (permitting discovery of any relevant, non-privileged material).

185. Pinkard v. Johnson, 118 F.R.D. 517, 520 (M.D. Ala. 1987) ("Any unwarranted restraints upon the process of newsgathering and reporting could jeopardize the free flow of information to the public.").

question before courts is whether "the paramount interest served by the unrestricted flow of public information protected by the First Amendment outweighs the subordinate interest served by the liberal discovery provisions . . . ."[186] In weighing these principles, courts identify a stronger interest in requiring disclosure for criminal proceedings,[187] but they have often held that even in civil cases, the circumstances may necessitate a reporter reveal information, including the identity of his sources.[188] Courts have thus strictly scrutinized such identification requests on news reporters.[189]

In civil cases, the test that has developed for analyzing a motion to quash a subpoena of a reporter who claims this qualified journalistic privilege requires the party seeking the subpoena to prove:[190] (1) the information sought is relevant; (2) there is no other means for obtaining the information or all other means have been exhausted; and (3) there is a compelling reason for disclosure.[191] Applying a case-by-case analysis, a court also examines the type of information sought in weighing the competing policies.[192] Thus, overly broad subpoenas may not pass the test because all information may not go to the core of the claim.[193] Moreover, information divulged by an informant under a promise of confidentiality may weigh in favor of non-disclosure.[194] In *Garland v. Torre*,[195] the Second Circuit Court of Appeals, for example, applied these principles holding that the reporter, who was also a named defendant, did not

186. Loadholtz v. Fields, 389 F. Supp. 1299, 1300 (M.D. Fla. 1975).

187. Baker v. F. & F. Investment, 470 F.2d 778, 785 (2d Cir. 1972); *see* Gilbert v. Allied Chem. Corp., 411 F. Supp. 505, 510 (E.D. Va. 1976) (stating the balance weighs differently for civil cases than it does for criminal, noting as one difference the ability of a civil litigant to explore several avenues to obtain the information he seeks).

188. Carey v. Hume, 492 F.2d 631, 637–39 (D.C. Cir. 1974) (requiring a journalist to reveal his source in a civil suit where the identity of the source went to the heart of the plaintiff's claim).

189. J.J.C. v. Fridell, 165 F.R.D. 513, 515–17 (D. Minn. 1995); Solarex Corp. v. Arco Solar, Inc., 121 F.R.D. 163, 167–75 (E.D.N.Y. 1988); *Loadholtz*, 389 F. Supp. at 1300.

190. Initially, the burden is on the reporter to show that the information sought was part of a newsgathering event. Von Bulow by Auersperg v. von Bulow, 811 F.2d 136, 144–45 (2d Cir. 1987). Then the burden switches to the party compelling discovery. *Pinkard*, 118 F.R.D. at 521.

191. *Pinkard*, 118 F.R.D. at 521; *see also* Los Angeles Mem'l Coliseum Comm'n v. Nat'l Football League, 89 F.R.D. 489, 494 (C.D. Cal. 1981) (discussing an analogous test).

192. *Pinkard*, 118 F.R.D. at 521.

193. Mere relevance is not sufficient. Rancho Pub. v. Superior Ct., 68 Cal. App. 4th 1538, 1549 (Cal. Ct. App. 1999); *see* Gulliver's Periodicals, Ltd. v. Chas. Levy Circulating Co., 455 F. Supp. 1197, 1204 (N.D. Ill. 1978) (holding the information sought could not be divulged because it did not go to the heart of the counterclaim).

194. Riley v. City of Chester, 612 F.2d 708, 714 (3d Cir. 1979).

195. 259 F.2d 545 (2d Cir. 1958).

have a First Amendment right to refuse to identify the source of the defamatory statements he published where the identification went "to the heart of the matter."[196] The court noted that privileged testimony is an extraordinary exception to the evidentiary rules and courts should err on the side of restricting the privilege rather than increasing it.[197] The subpoena in *Garland* was narrowly drafted, seeking only the identity of the anonymous source, thus, the court properly concluded that the balance tipped in favor of disclosure.[198] Narrowly drafted subpoenas on ISPs that seek only relevant, unprivileged information should likewise withstand attack in Internet defamation suits.

Despite the analogy this Comment advocates, the law does not *ipso facto* treat newspapers and the Internet equally. The Internet and newspapers differ as mediums in that a newspaper can be held liable for publishing defamatory remarks,[199] whereas an ISP cannot.[200] Although this Comment does not attack Congress's wisdom in granting immunity to ISPs for the content that they provide, at least one district judge has. Judge Friedman, of the D.C. Circuit Court of Appeals, recognized that an ISP, such as AOL, is much more like a newspaper than it is a common carrier like a telephone company.[201] Judge Friedman explained that, "[b]ecause it has the right to exercise editorial control over those with whom it contracts and whose words it disseminates, it would only seem fair to hold AOL to the liability standards applied to a publisher."[202] Moreover, because the news media is subject to liability, the potential for inaccuracies is decreased, while ISPs—which are immune from defamation liability—are more likely to publish untruths.[203] Internet speech in

196. *Id.* at 547, 550 (asking the court to deny the identification request on the ground that it "would, 'unreasonably annoy, embarrass, and oppress the deponent' "). *But cf.* Richards of Rockford, Inc., v. Pac. Gas & Elec. Co., 71 F.R.D. 388, 389 (N.D. Cal. 1976) (refusing disclosure of interviewing materials where the subpoena was issued to a non-party, there was no proof that defamatory statements were made during the interview, and the interview was for educational research); Mitchell v. Superior Ct., 690 P.2d 625, 632 (Cal. 1984) (stating identity disclosure in libel cases is not automatic).

197. Garland v. Torre, 259 F.2d 545, 550 (2d Cir. 1958).

198. *Id.* at 547.

199. Milkovich v. Lorain Journal, Co., 497 U.S. 1, 14–21 (1990). *But see* Zeran v. Am. Online, Inc., 958 F. Supp. 1124, 1132–37 (E.D. Va.), *aff'd*, 129 F.3d 327, 327 (4th Cir. 1997).

200. 47 U.S.C. § 230(e) (2000).

201. Blumenthal v. Drudge, 992 F. Supp. 44, 51 (D.D.C. 1998).

202. *Id.*

203. *See* LIPSCHULTZ, *supra* note 54, at 153 (arguing that although the Internet may increase the information available globally, this may not correspond to an increase in value).

general is, therefore, arguably of lesser value compared to that from reporters in other news media.[204] If true, this may cut in favor of courts revealing the identity of Internet posters even more readily than they do in the journalism cases. But asking courts to distinguish between the relative values of different forms of speech is walking a fine line of constitutionality.[205] Overall, these differences do not lessen the value of this analogy because these differences do not affect the important policies that courts must weigh in deciding whether to grant a subpoena to identify an unknown party. More specifically, in both instances, courts are balancing the right of anonymity and potential chill of speech against the entitlement for the state or any plaintiff to gain access to evidence.

CONCLUSION

Both ISPs and reporters are frequently served with subpoena motions asking them to reveal identifying information about alleged defamers.[206] Although the Internet as a medium for publication is unquestionably unique, subpoenas served on ISPs for identifying information of its users implicate the same policies as similar requests on reporters. Both analyses require a careful balancing of the right to speak anonymously and the potential chill if this right is infringed against the right for a plaintiff to have all relevant evidence when proceeding with litigation. Thus, a consistent standard for Internet defamation suits can be found in the test used in journalist cases.

The appropriate test is that a company, asking for identifying information from an online user's ISP, must prove that the information sought is relevant, goes to the heart of the company's claim, and is unavailable from any other source. This test requires a case-by-case determination that the plaintiff is, in good faith, bringing the subpoena only after exhausting other means of gaining the information itself. The plaintiff is not required to make a full, prima

204. *See* Lidsky, *supra* note 18, at 893 & n.195.

205. Larry Alexander, *Legal Theory: Low Value Speech*, 83 NW. U. L. REV. 547, 550 (1989) (asking if we really want to ask our courts to distinguish values of speech under the First Amendment and arguing that this would be quite problematic).

206. Subpoenas are issued to a variety of reporters, from those reporting for *The Washington Post* to reporters of small, local newspapers—most often these reporters are subpoenaed to identify criminals. Reporters Committee for Freedom of the Press, *Justice Releases Statistics on Subpoenas of Reporters*, (Dec. 6, 2001), *at* http://www.rcfp.org/news/2001/1206grassl.html (on file with the North Carolina Law Review). Likewise, AOL and other large ISPs say that responding to warrants and subpoena requests is like a full-time job. Stephen Dinan, *Search Warrants Keep AOL Busy*, WASH. TIMES, April 27, 1999, at C4, *available at* Lexis, Nexis Library, The Washington Times.

facie showing of defamation in this initial discovery request;[207] the plaintiff, however, must prove that the subpoena is narrowly drafted to ask only for information necessary to plead a legitimate claim of defamation. If the plaintiff can meet this burden, the court should order the subpoena on the ISP so the proper defendant can be identified.

MEGAN M. SUNKEL

207. *See* Dendrite Int'l, Inc. v. Doe, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001); *supra* notes 133–43 and accompanying text (discussing the plaintiff's burden).