UIC John Marshall Journal of Information Technology & Privacy Law

Volume 26
Issue 4 *Journal of Computer & Information Law - Summer 2009*

Article 2

Summer 2009

The Challenge of Internet Anonymity: Protecting John Doe on the Internet, 26 J. Marshall J. Computer & Info. L. 469 (2009)

Susanna Moore

THE CHALLENGE OF INTERNET ANONYMITY: PROTECTING JOHN DOE ON THE INTERNET

SUSANNA MOORE*

I. INTRODUCTION

The Supreme Court has consistently recognized that the First Amendment includes protection of anonymous speech.[1] There are many potential reasons to remain anonymous.[2] With the explosion of the Internet as an accessible and open forum for the exercise of free speech, however, the choice of many Internet users to remain anonymous on the Internet has tested the limits of the right to anonymous speech.[3]

As one commentator found, the Internet has become "ground-zero" in a battle over the right to speak anonymously within the protection of

* Clerk to the Honorable Leslie H. Southwick, U.S. Court of Appeals for the Fifth Circuit; Adjunct Professor, Mississippi College School of Law. All views expressed herein are the author's own.

1. Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 199-00 (1999) (invalidating state statute requiring initiative petitioners to wear identification badges); McIntyre v. Ohio Elections Comm., 514 U.S. 334, 341-42 (1995) (invalidating statute requiring election pamphlets to identify the author and comparing the decision to remain anonymous to "other decisions concerning omissions or additions to the content of a publication"); Talley v. California, 362 U.S. 60, 64 (1960) (invalidating statute prohibiting distribution of handbills without name and address of author).

2. *McIntyre*, 514 U.S. at 341-43 (1995). The Supreme Court listed some of these reasons in *McIntyre*: fear of retaliation or social ostracism; the desire to preserve privacy; the belief that an anonymous writing will be more persuasive; and to prevent the reader from being biased based on the writer's identity. *Id.*

3. It should be noted here that the term "Internet anonymity" is a sort of contradiction itself. Though the speaker's identity may be concealed from the typical Internet user, as Professor Jonathan Zittrain has pointed out, there are several Internet "points of control" where third parties can obtain identifying information: international gateways; Internet Exchange Points ("IXPs"); Internet Service Providers ("ISPs"); public access points (such as cybercafés, schools, or public libraries); corporate workplaces; technology service providers (such as blogging hosts, for instance); and other networks, like mobile and tracking devices such as Global Positioning Systems ("GPS") on vehicles or handheld devices. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

the First Amendment, largely because of its potential to contain defamatory or otherwise objectionable content.[4] Internet users communicate their ideas and opinions through a variety of means — blogs,[5] websites, and message boards[6] — and short of some cursory registration requirements, there are few restrictions on which Internet users may post their ideas, leading some to conclude that "the Internet is a democratic institution in the fullest sense."[7] Because of this accessibility and relatively small amount of censorship, the Internet is also a likely medium for defamation, which is not protected speech.[8]

Publication is an essential element of defamation,[9] and with the Internet, publication to millions can occur in an instant. The Supreme Court recognized the widespread audience one can reach through Internet communication in *Reno v. American Civil Liberties Union*:

> From the publishers' point of view, [the Internet] constitutes a vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers and buyers . . . Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of web pages . . . the same individual can become a pamphleteer.[10]

There are, however, certain downsides to instituting litigation against online defamers. First, it is statistically improbable that an individual, or a corporation to an even greater extent, will actually win a defamation suit.[11] Additionally, by bringing suit against the defamer,

---

4. Matthew S. Effland, *Digital Age Defamation: Free Speech Versus Freedom from Responsibility on the Internet*, 75 FLA. B. J. 63 (2001).

5. Blog is a contraction for "web log," which is defined by Merriam-Webster's Dictionary as "a Web site that contains an online personal journal with reflections, comments, and often hyperlinks provided by the writer." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 133 (11 ed. 2003).

6. Two popular message board sites are http://ragingbull.lycos.com and Yahoo!. Yahoo! maintains a message board for every publicly traded company, and any Yahoo! user may post messages on those boards. These posts are often a source of litigation. Other websites host message boards for people with common interests, from sports, to gardening, to health, to city-specific boards concerning community issues.

7. Brief for Public Citizen, Elec. Frontier Found., and Elec. Privacy Info. Ctr. as Amici Curiae, 2002 WL 32177985 at *5, Melvin v. Doe, 836 A.2d 42 (Pa. 2003).

8. See, e.g., Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942) (stating "it is well understood that the right of free speech is not absolute at all times and under all circumstances").

9. RESTATEMENT (SECOND) OF TORTS § 558 (1977).

10. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 853, 870 (1997).

11. According to one study, only thirteen percent of plaintiffs ultimately prevail in libel litigation. Randall P. Bezanson, et al., *The Economics of Libel*, *in* THE COST OF LIBEL: ECONOMIC AND POLICY IMPLICATIONS 21, 119 (Everette E. Dennis & Eli M. Noam eds., 1989). Public figure corporations were found to have succeeded only five percent of the time. *Id.* That is not to say, however, that it is impossible to win in such cases. For a list of suits

the plaintiff may actually be calling more attention to the alleged defamatory statements, where they might otherwise have gone relatively unnoticed. Furthermore, the plaintiff — particularly a corporate plaintiff — may be seen as a cruel Goliath in bringing suit against a single David Internet user. Another reason not to bring such suits in the context of Internet message or comment boards is that no statement on the board is given special preference, and any negative or untrue statement can be easily counteracted by a contradictory statement.[12]

In spite of these downsides, there has been a plethora of defamation, copyright infringement, and other litigation against anonymous Internet users.[13] Indeed, online critiques have proven to be such a concern for companies and individuals that some companies employ the use of private Internet monitoring services that monitor websites for communications about a company.[14]

The emphasis on protection from online defamation raises the question, then, about what is at stake in such litigation. One reason for the litigation may be the nature of the Internet is such that "[t]he extraordinary capacity of the Internet to replicate almost endlessly any defamatory message lends credence to the notion that 'the truth rarely catches up with a lie.'"[15] As one commentator found, "[a]t its best, the Net is the ultimate conduit for free speech and expression; at its worst, the Net can be a character assassin's greatest weapon."[16]

In instituting John Doe defamation litigation, more pernicious goals may, at times, be afoot. One commentator noted that, "[t]he sudden surge in John Doe suits stems from the fact that many defamation actions are not really about money."[17] Instead, she argued, such defamation suits are often brought to protect dignitary interests or to simply

---

against bloggers, along with the outcomes of those suits, *see* Media Law Resource Center, *Legal Actions Against Bloggers*, http://www.medialaw.org/Content/NavigationMenu/Hot_Topics/Lawsuits_Against_Bloggers/Lawsuits_Against_Bloggers.htm (last visited Feb. 5, 2010) (finding that several cases have gone to verdict against the bloggers, with combined awards in the amount of $16,128,280).

12. Contrast this to the newspaper forum, where a newspaper cannot feasibly be expected to print all responses or criticisms to every statement. Miami Herald Pub. Co. v. Tornillo, 418 U.S. 241, 256-57 (1974).

13. See cases *infra*, Part II.

14. Cyveillance, for example, offers Internet monitoring services directed at, among other things, "[i]nformation leaks and disgruntled employee activity," "[p]lans to disrupt events or harm employees," and "[s]ales and distribution of personal credentials." Cyveillance, http://www.cyveillance.com/ (last visited Feb. 5, 2010).

15. Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L. J. 855, 864 (2000) (quoting Gertz v. Robert Welch, Inc., 418 U.S. 323, 344 n.9 (1974)).

16. Elfand, *supra* note 4.

17. Lidsky, *supra* note 15, at 872.

make the speech cease.[18] In this context, the potential chilling of speech is a legitimate First Amendment concern.[19] It is for this reason that the protection of John Doe's anonymity is essential.

The question of what tests courts should use in deciding whether to reveal the identities of anonymous Internet users is unsettled. Part II of this Article will discuss the various tests courts have applied in determining whether the identity of an anonymous Internet user should be revealed — including a good-faith test, a summary judgment standard, and a balancing test. Part III will analyze the merits of each test. Part IV will conclude by recommending the appropriate test courts should use in deciding whether to reveal the identities of anonymous Internet users.

II. THE DIFFERENT TESTS USED TO DETERMINE WHETHER TO UNMASK AN ANONYMOUS BLOGGER

When a party learns that he has potentially been defamed or his copyright infringed on the Internet, he may choose to institute a litigation proceeding — either by filing a complaint or initiating a proceeding for pre-litigation discovery.

If the alleged defamer or infringer is anonymous, the party would seek to discover the identity of the individual. The potential plaintiff may seek to do this in a number of ways. If the website where the offending material is found has a registration component to it, the plaintiff may ask the website for the information the party provided at registration. In combination or in the alternative, the party may seek to find out the user's Internet Protocol ("IP") address from the Internet service provider ("ISP"). An IP address is a number that identifies a device that is communicating with the Internet.[20] If a computer uses a "static" IP address, it uses the same IP address each time it connects to the Internet; a computer with a "dynamic" IP address receives a new number out of a pool of

18. In this context, it has been proposed that such John Due suits should be considered under anti-SLAPP (Strategic Lawsuits Against Public Participation) laws. *See e.g.*, Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261 (C.D. Cal. 2001); 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 (2001); Shaun B. Spencer, *Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493 (2001).

19. In one case where the court refused to enforce subpoena unmasking anonymous Internet users where the John Does were nonparties, the court found that "[i]f Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights." Doe v. 2theMart.com, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

20. Michael J. Tonsing, *A Fashion Model, A Mean-Spirited Name-Calling Detractor, a Blog, and at Least Four Teachable Moments*, 56 FED. LAW. 10, 10 (Oct. 2009).

numbers, generally for each new Internet session.[21] The plaintiff would seek to first identify which IP address posted the offending information. He may require a subpoena to get this information. If he could obtain that information, he would then attempt to determine which computer was associated with that IP address by contacting the ISP. This too may require a subpoena.[22]

The plaintiff will seek to compel disclosure by the ISP of the identity of the user associated with the IP address. According to two practicing attorneys, the subpoena should be relatively broad and ask for logs of the "times, dates, and places of the alleged defamatory postings" as well as personal information about the poster of the statements, such as his "name, address, and telephone number."[23] The plaintiff will not name the ISP as a defendant because the Communications Decency Act protects the ISPs from such liability.[24]

At this point, the precise response will depend on the policies of the ISPs and the jurisdictions where the suit is filed. Generally, the ISP will notify the user and will not provide any legal services to the user, because "[f]or Yahoo, or any other ISP, to step in and offer legal help for their members would cost them a huge amount in legal fees."[25] Depending on the jurisdiction, however, notification may not be required and may not thus occur. The different approaches taken by courts in analyzing whether to compel the disclosure of John Doe's identity range anywhere on the spectrum from applying a good-faith standard to a five-part test, including a balancing test, and are discussed in the following sections.

A. The Good-Faith Standard

The least exacting standard set by courts has been the so-called "good-faith standard" of *In re Subpoena Duces Tecum to America Online, Inc.*[26] In that case, an anonymous plaintiff company sued five unknown individuals alleging that they had published defamatory and confidential

21. *Id.* This is a simplification of the options; however, a detailed description of the terminology and technology is beyond the scope of this article.

22. Because of such litigation, Internet service providers have been "bombarded" with such requests. Jeffrey Terraciano, *Can John Doe Stay Anonymous?*, Wired.com, Feb. 21, 2001, http://www.wired.com/politics/law/news/2001/02/41714 (last visited Feb. 5, 2010).

23. Roger Rosen & Charles Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, 24 L.A. Law. 19, 19 (Oct. 2001).

24. 47 U.S.C. § 230(c) (2000) (providing that the Internet service provider should not be treated as the author of the material, even when it is published through its services, and thus cannot be sued for defamation).

25. *See* Terraciano, *supra* note 22.

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

material in Internet chat rooms.[27] The suit was first brought in Indiana, and the Indiana court issued an "Order Authorizing Plaintiff To Conduct Discovery In Virginia And Requesting Assistance Of State Of Virginia Trial Courts To Issue Subpoena In Support Of Indiana Discovery."[28] America Online then filed a motion to quash the subpoena or, in the alternative, a protective order from the Virginia court.[29]

The court examined the Indiana pleadings and the Internet postings at issue to determine whether the subpoena should be granted.[30] Ultimately, the court held that three requirements must be in place for the identity of an anonymous defendant to be revealed.[31] First, the court must be "satisfied by the pleadings or evidence supplied to that court."[32] Second, the requesting party must have a "legitimate, good faith basis" that the conduct was actionable.[33] Third, the identifying information must be "centrally needed" to advance that claim.[34]

The court did not provide any guidance as to what the phrase "satisfied by the pleading or evidence supplied to that court" is to mean to courts interpreting its decision. However, based on the language of the court's decision, whatever "satisfied by the pleading or evidence" means, it likely does not mean a substantive weighing of the merits of the plaintiff's arguments. Ultimately, the court found that the compelling state interest of protecting citizens from the harmful effects of such Internet communications outweighed any "limited intrusion" on the First Amendment rights of the John Doe Internet users.[35]

B. Motion to Dismiss / Prima Facie Case Standards

Other courts have applied more vigorous standards before allowing John Doe's identity to be revealed. An important case requiring more of a showing of evidence by the plaintiff before anonymity is broken is *Columbia Insurance Co. v. Seescandy.com*, where the Northern District of California addressed whether it should allow limited discovery so that

27. *Am. Online I*, 52 Va. Cir. at 27.
28. *Id.*
29. *Id.*
30. *Id.* at 29. Since the Indiana ruling was not a final judgment, the Full-Faith and Credit Clause did not apply. *Id.* (citing *Baker v. Gen. Motors Corp.*, 522 U.S. 222 (1998)). The court recognized the importance of the principle of comity, but found that it would not "blindly defer to a ruling of another court which could substantially abridge the constitutional rights of the John Does." *Id.* at 27. Comity did, however, constrain the court's consideration of the issue of whether the plaintiff should be allowed to proceed anonymously for a limited period of time. *Id.* at 27-28.
31. *Am. Online I*, 52 Va. Cir. at 37.
32. *Id.* at 29.
33. *Id.*
34. *Id.*
35. *Id.* at 29-30.

the plaintiff could ascertain the defendant's identity and thus issue service.[36] In that case, an unknown defendant had registered an Internet domain name, seescandy.com, which the plaintiff, the assignee of the federally registered service and trademarks "See's" and "See's Candies," claimed constituted dilution and trademark infringement.[37]

In *Seescandy*, the court outlined a four-prong approach to determine whether the identity of a defendant should be revealed under those circumstances, requiring: (1) specific identification of the party; (2) a showing of a good faith effort to locate the individual and comply with the requirements of service of process; (3) that the plaintiff could withstand a motion to dismiss;[38] and (4) a discovery request stating the reason for the request, identifying the individuals on whom discovery process might be served and showing a reasonable likelihood that the discovery process will lead to identifying information about the defendant.[39] There was no full merits consideration, though the merits were considered to the extent necessary to determine whether the plaintiff could withstand a motion to dismiss.[40]

In *Sony Music v. Does 1-40*, a New York federal case applied a standard very similar to that in *Seescandy* in addressing whether the identity of alleged copyright infringers should be revealed so that a claim for illegal use of file-sharing programs should proceed.[41] As a threshold matter, the court in *Sony Music* determined whether the sharing and downloading of files was an exercise of speech.[42] The court concluded that it was, "but only to a degree."[43] The court explained that a file sharer may express himself through the music that he selects and shares with others.[44] Ultimately, the court found that this was First Amendment speech entitled to some protection, even if not "political speech" entitled to the "broadest protection."[45]

---

36. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 575 (N.D. Cal. 1999).

37. *Id.*

38. The court found that the "plaintiff must make some showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed that act." *Id.* at 580.

39. *Id.* at 578-80.

40. *Id.* at 580 (citing AMF, Inc. v. Sleekcraft Boats, 599 F.2d 341 (9th Cir.1979)). In analyzing the third prong, the court considered the test for infringement of a federally registered trademark and for false designation of origin under the Lanham Act, i.e. whether the act in question creates a likelihood of confusion. The court applied the factors identified by the Ninth Circuit to answer this question, finding there to be sufficient likelihood of confusion, rendering the plaintiff capable of surviving a motion to dismiss.

41. Sony Music Entm't, Inc. v. Does 1-40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

42. *Id.* at 558.

43. *Id.* at 564.

44. *Id.*

45. *Id.*

The court in *Sony Music* borrowed from the tests developed by the courts in *America Online*, *Seescandy*, *Dendrite International, Inc. v. Doe*, and *In re Verizon Internet Services, Inc*.[46] The court culled together parts of those cases and treated them as nonexclusive factors.[47] The factors in *Sony Music* included: (1) "a concrete showing of a prima facie claim of actionable harm;[48] (2) specificity in the discovery request;"[49] (3) lack of alternative means to obtain the information sought by the subpoena;[50] (4) "a central need" for the information sought by the subpoena;[51] and (5) the defendant's expectation of privacy.[52]

Certain aspects of the *Sony Music* approach may make it seem less protective than *Seescandy*. For one thing, what were elements in *Seescandy* were merely factors in *Sony Music*. Further, though there is an additional factor of expectation of privacy, that factor can be cursorily dealt with in most of such cases.[53] On the other hand, the "concrete showing" of a valid *prima facie* claim may involve a merits determination more rigorous than the motion to dismiss standard of *Seescandy*. Additionally, the initial weighing of the First Amendment interests at play, though the court did not expressly indicate how such weighing should occur in future cases, indicates a sort of balancing of the interests involved.[54] In *Sony Music*, the court found the act of downloading and sharing music to be an expression of speech, but since it lacked political

46. *Id.* at 564-65.

47. *Sony Music*, 326 F. Supp. 2d at 564-65.

48. *Id.* at 564-65 (citing *Seescandy.com*, 185 F.R.D. at 577, 579-81; *Am. Online I*, 52 Va. Cir. at 28; Dendrite Int'l, Inc. v. Doe, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

49. *Sony Music*, 326 F. Supp. 2d at 565; *McIntyre*, 514 U.S. at 565 (1995) (citing *Seescandy.com*, 185 F.R.D. at 578, 580); *Dendrite*, 775 A.2d at 760.

50. *Sony Music*, 326 F. Supp. 2d at 565 (citing Seescandy.com, 185 F.R.D. at 579).

51. *Id.* at 565 (citing Am. Online, v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 381 (Va. 2001); *Dendrite*, 775 A.2d at 760-61).

52. *Id.* (citing *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 260-61, 267-68 (D.D.C. 2003), *rev'd on other grounds*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Serv., Inc., 351 F.3d 1229 (D.C. Cir. 2003)).

53. Service provider agreements will often lower any expectation of privacy by their terms. In *Sony Music*, the court examined Cablevision's Terms of Service, to which the defendants agreed, finding that it prohibited the "[t]ransmission or distribution of any material in violation of any applicable law or regulation . . . This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization." *Sony Music*, 326 F. Supp. 2d at 566. The Terms of Service also stated that "Cablevision has the right . . . to disclose any information as necessary to satisfy any law, regulation or other governmental request." *Id.* The Cablevision agreement in that case, just like the Yahoo! service agreement *infra*, II.D, grants broad discretion to the holders of the anonymous user's information to reveal that information in response to legal action, thus eviscerating the user's expectation of privacy.

54. *Sony Music* could potentially be seen as a precursor to *Dendrite*, *infra* II.D, though the effect and importance of this balancing is not as clear in *Sony Music* as it is in *Dendrite*, where the court was more explicit.

value it was not given the greatest protection.[55] A future court applying *Sony Music* to speech deemed political speech would certainly have to apply the factors much more rigorously.

C. The Summary Judgment Standard of Doe v. Cahill

The Delaware Supreme Court, *Doe v. Cahill*, adopted a more exacting approach than the *prima facie* cases.[56] In *Cahill*, a public official sought to compel an ISP to unmask an online critic based on alleged defamatory statements criticizing the plaintiff's performance as city councilman.[57] The court found that in order for a defamation plaintiff to obtain the identity of an anonymous defendant through the compulsory discovery process he must support his defamation claim with facts sufficient to defeat a summary judgment motion.[58]

While the court in *Cahill* declined to adopt the *Dendrite* approach[59] in its entirety, in addition to the summary judgment standard, the *Cahill* court adopted the first step of *Dendrite*: the notification provision.[60] In declining to adopt the final step in *Dendrite*: the balancing test, the court found that "[t]he summary judgment test is itself the balance" and that the balancing step "adds no protection above and beyond that of the summary judgment test and needlessly complicates the analysis."[61]

The approach in *Cahill* has been followed by several other courts. For example, a California Appellate Court, in *Krinsky v. Doe 6*, followed *Cahill* over *Dendrite*, though with some alterations.[62] For instance, while maintaining that notification should be required, the court did not require notice by way of a posting on the original forum about the lawsuit, finding such a requirement futile because "an Internet Web site, chat room, or message board may no longer exist or be active by the time the plaintiff brings suit."[63]

---

55. *Sony Music*, 326 F. Supp. 2d at 564.

56. Doe v. Cahill, 884 A.2d 451 (Del. 2005).

57. The comments appeared on a web page called the "Smyrna/Clayton Issues Blog," which allowed for users to post about local issues. *Id.* at 454. At the top of the blog, under "Guidelines," it read "[t]his is your hometown forum for opinions about public issues." *Id.*

58. *Cahill*, 884 A.2d at 460.

59. *See infra*, II.D.

60. *Cahill*, 884 A.2d at 460 (finding that notification imposes "very little burden on a defamation plaintiff," and furthermore in the First Amendment context, the court "disfavor[s] ex parte discovery requests that afford the plaintiff the important form of relief that comes from unmasking an anonymous defendant").

61. *Id.* at 461.

62. Krinsky v. Doe 6, 159 Cal. App. 4th 1154, 1170-72 (Cal. App. 2008).

63. *Id.* at 1171

D. The Dendrite Balancing Approach

Of the tests employed by courts, the most protective of the First Amendment is the one adopted by the New Jersey Superior Court Appellate Division in *Dendrite International, Inc. v. Doe*.[64] Yahoo! is an Internet company that provides services such as e-mail, search engines, and bulletin and message boards.[65] As a publicly traded company, Dendrite, a company that developed and serviced software for the pharmaceutical industry, had a bulletin board devoted to it on Yahoo! Finance.[66]

Dendrite alleged that on the bulletin board were several postings that constituted breaches of contract, defamatory statements, and misappropriated trade secrets.[67] The terms of service agreement to which the John Does agreed when they signed up for Yahoo!'s services provided very little protection for the user's identity vis-à-vis Yahoo!:

> As a general rule, Yahoo! will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believe in good faith that the law requires it or under the circumstances described below . . . Yahoo! may disclose account information in special cases where we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating Yahoo!'s Terms of Service or may be causing injury to . . . anyone . . . that could be harmed by such activities.[68]

In *Dendrite*, the court set out a five-part standard for when courts should order the identity of John Doe defendants to be revealed. First, the court should require the plaintiff to attempt to notify the anonymous posters that they are subject to a subpoena or application for disclosure.[69] Second, the court should require the plaintiff to identify the exact statements that allegedly constitutes actionable speech.[70] Next, the court should determine whether the plaintiff has set forth a *prima facie* cause of action against the John Doe defendants.[71] The plaintiff must produce an evidentiary basis for each element of the cause of action.[72]

---

64. *Dendrite*, 775 A.2d 756.

65. *Id.* at 761.

66. *Id.* at 761-62.

67. *Id.* at 763.

68. *Id.* at 762. Yahoo! could, of course, choose to protect its users' identities as vigorously as it chooses to do. However, the terms of the agreement, with its good-faith standard, sets the bar very low for its mandatory responsibilities.

69. *Id.* at 760. The purpose of this requirement is to give the John Doe defendants the opportunity to oppose the application. This notification may in the Internet context include a posting about the defamatory action on the original message board.

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

71. *Id.* In making this determination, the court should review the complaint and all information provided to the court. *Id.*

72. *Id.*

Finally, the court should balance the defendant's First Amendment right to anonymous free speech against the strength of the *prima facie* case the plaintiff has presented and the necessity of the disclosure of the defendant's identity in order for the plaintiff's action to properly proceed.[73] In *Dendrite*, the court ultimately concluded that two of the four John Doe defendants should remain anonymous.[74]

The *Dendrite* court laid a clear test for other courts to follow, and this position was solidified by the same court in *Immunomedics, Inc. v. Doe*, handed down the same day as *Dendrite*.[75] In that case, the plaintiff, a biopharmaceutical corporation, brought action against a John Doe Internet user. The John Doe was believed to be an Immunomedics employee based on statements made on a Yahoo! message board, and Immunomedics alleged that the statements constituted breach of a confidentiality agreement.[76] The court repeated verbatim its language from *Dendrite*, making clear that its *Dendrite* holding has the same force in a breach of contract claim.[77]

The *Dendrite* standard has been adopted by several courts[78] and has been supported by numerous commentators.[79] For example, in *Mobilisa, Inc. v. Doe*,[80] a case involving unlawful access to e-mail communications, an Arizona court supported the reasoning of *Cahill* and *Dendrite* but ultimately adopted the *Dendrite* balancing test, finding the balancing test necessary for three reasons. First, the court found the balancing step "necessary to achieve appropriate rulings in the vast array of factually distinct cases likely to involve anonymous speech."[81] Second, the court found the balancing consistent with the standard for examining prelimi-

---

73. *Id.*

74. *Id.*

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

76. *Id.* at 774.

77. *Id.* at 777.

78. *See infra* part IIIB.

79. *See e.g.*, Larissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537 (2007); Jennifer O'Brien, Note, *Putting a Face to a Screen Name: The First Amendment Implications of Compelling ISP's to Reveal the Identities of Anonymous Internet Speakers in Online Defamation Cases*, 70 FORDHAM L. REV. 2745 (2002); Margo E.K. Reder & Christine Neylon O'Brien, *Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking the Identity of Anonymous Employee Internet Posters*, 8 MICH. TELECOMM. & TECH. L. REV. 195 (2002); Furman, *supra* note 18; Spencer, *supra* note 18.

80. Mobilisa, Inc. v. Doe, 170 P.3d 712 (Ariz. Ct. App. 2007).

81. *Id.* at 720. For example, the court found that without the balancing test, the reviewing court would not be able to consider important factors including "the type of speech involved, the speaker's expectation of privacy, the potential consequence of a discovery order to the speaker and others similarly situated, the need for the identity of the speaker to advance the requesting party's position, and the availability of alternative discovery methods." *Id.* (footnote omitted).

nary injunctions,[82] which the court found analogous.[83] Third, the court found that this additional step was consistent with the broad protection for free speech and individual privacy provided under the Arizona constitution.[84]

Similarly, in *Highfields Capital Management v. Doe*, a California court required that after defeating a motion for summary judgment, the plaintiff must then pass a balancing test where the court will "assess and compare the magnitude of the harms to the competing interests by a ruling in favor of plaintiff and by a ruling in favor of defendant."[85] The court made no mention, however, of *Dendrite*'s notification requirement.

In a recent Maryland case, the court adopted the *Dendrite* approach, concluding that the John Does' identities should have been protected.[86] There, defendants had posted alleged defamatory material on a forum discussion allowing for discussion of local issues in Centreville, Maryland.[87] Under the "Centreville Eyesores" discussion thread, users alleged the intentional burning of plaintiff's home by its buyer and that plaintiff's food-service establishment was unsanitary.[88] To post on the site, users were required to register with an e-mail address, and the terms of the user agreement did not guarantee the protection of anonymity.[89]

The court examined the various approaches by other courts on the issue and the competing interests implicated in such cases. Ultimately, it concluded that the *Dendrite* approach "most appropriately balances a speaker's constitutional right to anonymous Internet speech with a

---

82. In order to obtain a preliminary injunction, the requesting party must show that a balance of hardships favors it (considering factors such as a strong likelihood of success on the merits, the possibility of irreparable injury, and public policy). *Id.* at 720-21 (citing Shoen v. Shoen, 804 P.2d 787, 792 (Ariz. Ct. App. 1990)).

83. *Mobilisa*, 170 P.3d at 720-21.

84. *Id.* at 721 (citing ARIZ. CONST. art. 2, §§ 6 & 8; Mountain States Tel. & Tel. Co. v. Ariz. Corp. Comm'n, 773 P.2d 455, 459-60, 462 n. 13 (1989)).

85. Highfields Capital Mgmt. v. Doe, 385 F. Supp. 2d 969, 976 (N.D. Cal. 2005).

86. Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432 (Md. 2009).

87. *Id.* at 442-45. The Internet forum discussion was hosted by Independent Newspapers on its website Newszap.com. *Id.* at 443 n.12. At the time of this publication, under the logo of Newszap.com is the text "Free Speech" and "Free Ads." *See* Newsap.com, http://www.newszap.com (last visited Feb. 5, 2010).

88. The exact content of the alleged defamatory speech is quoted in the opinion. *Brodie*, 966 A.2d at 440-43.

89. The following was stated in the privacy policy:

> While we preserve one's right to anonymity on the forum pages, we do require each individual to register a user name, email address, and password. This protects newszap.com AND the individual from false representations. Individuals posting libelous or defamatory comments are not welcome at this site and are granted no right to anonymity should a court of law seek a poster's identity. *Id.* at 444 n.13.

plaintiff's right to seek judicial redress from defamatory remarks."[90]

III. ANALYSIS OF THE STANDARDS

A. Arguments against Heightened Standards for Internet Defamation Defendants

Some commentators may criticize the effects of any sort of heightened requirements for plaintiffs seeking redress for wrongs done to them on the Internet. One criticism is that it does not make sense to provide an anonymous Internet defamer more protection than an anonymous author of a book or pamphlet when the Internet has the capability of reaching so many people.[91] Moreover, the Internet has more permanence than other forms of communication, in that any Internet user can use a simple search to find a defamatory statement years after its initial publication.

Put simply, the crux of these criticisms is that *Dendrite* and similar cases go too far. "While the First Amendment right to speak anonymously is 'well-established,' it does not necessarily require broad procedural protections in the John Doe context."[92] Such criticisms distinguish much of the Supreme Court precedent cited in cases like *Dendrite* and *Cahill* because those involve prior restraints, noting that the court has found that First Amendment rights are not absolute.[93]

Another concern is that during discovery, the plaintiff may need to know the identity of the defendant in order to know if he can or should proceed in the matter. First, under the *Cahill* and *Dendrite* standards, a plaintiff must be able to establish all the elements of the cause of action. In certain circumstances, however, the plaintiff may not be able to establish the elements of the cause of action without knowing the identity of the defendant. For example, if the claim is based on a breach of an employment contract, the plaintiff may not be able to establish that the John Doe defendant is in fact an employee of the corporation without establishing his identity. In the defamation context, if "actual malice" is a required element of defamation claim, the identity of the defendant may be necessary in order to pass the summary judgment stage.[94] At least one court has recognized this as a valid concern.[95]

---

90. *Id.* at 456.

91. *See, e.g.*, O'Brien, *supra* note 78, at 2764-65.

92. Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing Over Legal Standards*, 83 Or. L. Rev. 795, 808 (2004).

93. *Id.* at 808.

94. Melvin v. Doe, 836 A.2d 42, 46 (Pa. 2003).

95. Melvin v. Doe, 49 Pa. D. & C.4th 449, 453 (Pa. Comm. Pl. 2000), *appeal quashed on other grounds*, 789 A.2d 696 (Pa. Super. Ct. 2002), *rev'd*, 836 A.2d 42 (Pa. 2003).

> [P]laintiff needs to know the identity of the Doe defendants prior to incurring the expenses and other burdens of a trial, because it is questionable whether plaintiff

Similarly, without knowing the identity of the defendant, the plaintiff cannot know if certain jurisdictional requirements have or will be met. If the plaintiff wishes to establish jurisdiction based on diversity of citizenship, he will have no way of knowing for certain the state of citizenship of the defendant and courts may be reluctant to hear the case.[96] With regard to the issue of personal jurisdiction, one commentator has found that, "[t]he judicial trend is a 'sliding scale' for the evaluation of the defendant's contacts" whereby the court considers "both the quality and quantity of the entity's online activity to determine if it may constitutionally exercise personal jurisdiction."[97]

Michael S. Vogel, attorney for Dendrite in *Dendrite, Intl. v. Doe*, has criticized the *Dendrite* and *Immunomedics* court's approach for the amount of discretion that it place in the hands of trial judges.[98] His article points out that the judge's determination at the discovery phase can amount to a final judgment for defamation plaintiffs, which may not be appealable as of right as an interlocutory order or which may be reviewed for an abuse of discretion.[99] The result, according to Vogel, is the risk of "transforming our elaborate judicial system—with the time-tested due process rights it affords—into an unregulated judicial 'gut check' as to the merit or importance of a particular plaintiff's claim."[100] At least one court has explicitly agreed with Vogel's statement that "the new standards offer little real protection for anonymous speech beyond what

---

would wish to proceed with a trial if John Doe turned out to be, for example, an inmate incarcerated pursuant to a trial before plaintiff. In this instance, it is unlikely that any judgment that she obtained would be satisfied. *Id.*

96. *See* Macheras v. Center Art Galleries-Hawaii, Inc., 776 F. Supp. 1436, 1440 (D. Haw. 1991) (stating "[a] plaintiff who names Doe defendants, files suit in federal court at his peril"); Salzstein v. Bekins Van Lines, Inc., 747 F. Supp. 1281, 1283 (N.D. Ill. 1990) (disfavoring granting of diversity jurisdiction in Doe defendant cases); W. Weber Co. v. Kosack, 1997 U.S. Dist. LEXIS 16786 at *7-9 (S.D.N.Y. Oct. 24, 1997) (denying defendant's motion to dismiss for lack of subject matter jurisdiction, noting the struggle that federal courts face in determining whether unknown parties meet the requirement of diversity jurisdiction).

97. Meagan M. Sunkel, Comment, *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*, 81 N. C. L. REV. 1189, 1202 (2004) (citing Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997)).

98. Vogel, *supra* note 91, at 809.

99. *Id.* at 809-10 & n.70 (comparing the rule of New York, which does not permit routine appeal of interlocutory orders, N.Y. C.P.L.R. § 5701(a) (McKinney 1995 & Supp. 2005), to the Pennsylvania rule, where John Doe discovery orders are appealable as of right under Pennsylvania's collateral order rule, Pa. R. App. P. 313, Melvin v. Doe, 836 A.2d 42, 44 (Pa. 2003)). Vogel noted that the "appealability of such an order could likely be resolved differently by different states, under different appellate rules." *Id.* at. 810 n.10.

100. *Id.* at 810.

the courts can provide under existing rules."[101]

B. The Dendrite Standard Provides the Best Test for Unmasking Anonymous Internet Users

The test provided by the *Dendrite* court, with its measured approach and flexibility, is the best approach to such cases. Moreover, the *Dendrite* test does not go too far in its protection, as some critics suggest, for its standard is far from insurmountable for plaintiffs. This is borne out by the fact that two of the anonymous defendants' identities were ultimately ordered to be revealed in *Dendrite*.[102] Additionally, in the companion case to *Dendrite*, the court found that the anonymous defendant's identity should be revealed.[103]

The first step of *Dendrite*, the notification provision, which was also adopted by the Court in *Cahill*, is a necessary provision for the protection of anonymous Internet speech. The right to anonymous speech is constitutionally protected, and ISPs and web hosts should not be entrusted with protecting that right on behalf of the Internet user. Without a notification requirement, John Doe defendants who wish to remain anonymous may not stand a fighting chance.

As the courts in *Dendrite* and *Cahill* noted, the burden and costs associated with notification are relatively low, particularly in relation to the potential high costs implicated in the First Amendment context. As a practical matter, it is a relatively simple task to notify the user of the suit and give him an opportunity to remain anonymous. A mere e-mail or online message would suffice.

To the extent that there is any burden at all, ISPs cannot be expected to carry the burden of notification on behalf of their users without a clear mandate or incentive to do so. Though there may be some economic incentive for ISPs to protect users' information,[104] that incentive cannot be relied on as sufficient to protect users' identities. At least one commentator has found this incentive insufficient, noting that, "companies targeted by anonymous online critics have thus tended to view ISPs and operators of online message boards as allies rather than adversa-

101. Klehr Harrison Harvey Branzburg & Ellers, LLP v. JPA Dev., Inc., No. 0425, 2006 WL 37020 at *8 (Pa.Com.Pl. Jan. 4, 2006) (quoting Vogel, *supra* note 91, at 801). This case actually involved plaintiffs who had already been identified and were opposing a discovery order requesting the identify of specific posters of information on a website.

102. *Dendrite*, 775 A.2d at 772.

103. *Immunomedics*, 775 A.2d 773.

104. There may, however, be some economic incentive to protect user information, where a company may excel in the free market by becoming known as a company that takes pride in protecting user information.

ries."[105] In light of the lack of clear incentive to notify or otherwise protect users, courts should mandate notification.

The next steps in the *Dendrite* test relate to the specificity and sufficiency of the plaintiff's case. The plaintiff must identify the exact statements that are allegedly actionable. The plaintiff must also establish an evidentiary basis for each element of the cause of action.

These steps give adequate consideration to the interests of the parties on both sides. The analysis prevents John Doe from being identified where the case has no likelihood of success. On the plaintiff's side, the analysis provides that the merits of the case will get some consideration at this level. Concerns like those mentioned above (i.e. that by denying the plaintiff the right to learn John Doe's identity a final judgment may ignore the merits of the evidence) are actually considered under the *Dendrite* approach.

The last step of *Dendrite*, the balancing test, is well-suited to John Doe Internet cases because it provides the greatest flexibility. The Internet is a versatile medium, and anonymous speech cases arising under the Internet can vary greatly. As the court in *Highfields* found, the balancing test is the one most adequate to address the broad range of types of speech such cases can involve.[106] Moreover, the *Dendrite* balancing test is preferable because as one commentator found, "[m]erely requiring the complaint to survive a motion to dismiss does not sufficiently protect John Doe's anonymity."[107] As in *Dendrite* itself, even where a claim may survive a Rule 12(b)(6) motion, it may be destined to fail on its factual merits. The balancing test bridges this gap, addressing the difference between legally stating a claim and having a case that has actual likelihood of success.

IV. CONCLUSION

The Internet has undeniably changed the way people communicate ideas and express themselves. As Internet technology and accessibility has rapidly expanded, courts have struggled with how existing First Amendment principles should be applied. In the context of determining whether to unmask the identity of anonymous Internet users, this struggle has resulted in inconsistent results in the courts. The approaches courts use to determine whether to unmask the identity of John Does on the Internet range from those that severely threaten First Amendment rights to those that are more protective of First Amendment concerns.

105. Bruce P. Smith, *Cybersmearing and the Problem of Anonymous Online Speech*, 18 COMM. LAWYER 3, 6 (Fall 2000).

106. *See supra* part IIID.

107. Spencer, *supra* note 18, at 517-18.

In these John Doe cases, courts must grapple with important competing interests. Plaintiffs have a right to address actionable speech in the courts, and defendants have a right to speak anonymously. The *Dendrite* test is the approach that best addresses both of these interests. First, it gives the John Doe defendant the notification necessary to protect his anonymity. It also provides that the plaintiff's case must have some merit, so that John Doe will not be unmasked for the sake of a meritless case. The balancing test insures that anonymity may stand where there is low likelihood of plaintiff's success or where the unmasking is not necessary to proceed.

Without the protection provided in cases like *Dendrite*, users of the Internet will suffer from dangerous chilling effects. The traditional right to anonymous speech, long recognized by the Supreme Court, must not fall by the wayside simply because technology has changed the channels of speech. As the Supreme Court has recognized, an Internet connection and a computer can turn any individual into the town crier or pamphleteer of bygone days. The First Amendment interests in online communications are no different from those in the Supreme Court's cases involving "traditional" methods of communication. As technology changes the methods of expression, courts must ensure that First Amendment protections keep pace.