UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 3 *Journal of Computer & Information Law - Spring 2001*

Article 3

Spring 2001

Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace, 19 J. Marshall J. Computer & Info. L. 493 (2001)

Shaun B. Spencer

CYBERSLAPP SUITS AND JOHN DOE SUBPOENAS: BALANCING ANONYMITY AND ACCOUNTABILITY IN CYBERSPACE

by SHAUN B. SPENCER†

Lawyers in so-called "cyberSLAPP"[1] lawsuits frequently subpoena Internet Service Provider ("ISP") records to expose the authors of anonymous Internet postings. This trend pits two legitimate interests against one another.[2] The anonymous poster—John Doe[3]—claims a First Amendment right to participate anonymously in public debate. On the other hand, companies want John Doe held accountable when his postings harm them.

Current law favors accountability at the expense of anonymity. John Doe often receives no meaningful notice before his ISP discloses his identity to the very company from whom he wanted to remain anonymous. Additionally, existing law allows a cyberSLAPP plaintiff to pierce John Doe's anonymity at the outset of the case, with no judicial oversight to determine whether the plaintiff has a substantial claim.

This article proposes an amendment to the *Electronic Communications Privacy Act* ("ECPA") to restore the balance between anonymity and accountability. The amendment ensures that before the ISP discloses John Doe's identity, John Doe will have had notice and an opportunity to appear through counsel at a hearing where a court reviews the subpoena. The amendment also requires a judicial finding that the

---

† Climenko/Thayer Lecturer on Law, Harvard Law School. I am grateful for the contributions of Lawrence Friedman, Megan Gray, Paul Levy, and Lyrissa Lidsky. I thank Megan Gray for suggesting the term, "cyberSLAPP" to me.

1. George Pring, *SLAPPs: Strategic Litigation Against Public Participation*, 7 Pace Envtl. L. Rev. 3, 4 (1989). The term "cyberSLAPP" is a variation on the acronym SLAPP, which stands for strategic litigation against public participation. *Id.* SLAPP suits are actions brought by large private interests "to stop citizens from exercising their political rights or to punish them for having done so." *Id.* at 5–6. The typical "cyberSLAPP" is a suit brought to punish or deter anonymous online criticism. *Id.*

2. *See id.*

3. Though the anonymous poster can be either male or female, I shall refer to the hypothetical anonymous poster in this article as "John Doe."

plaintiff has sufficient evidence to prove a prima facie case and that the plaintiff's need for John Doe's identity outweighs John Doe's interest in anonymity. This careful judicial review will prevent the needless intrusion on John Doe's First Amendment interest in anonymity, while preserving a remedy for those legitimately harmed by anonymous online speech.

I. THE RISE OF CYBERSLAPP LAWSUITS

The late 1990s witnessed the democratization of securities trading and a booming stock market.[4] These phenomena popularized online financial discussion boards and chat rooms, such as those hosted by Raging Bull, Yahoo!, Motley Fool and Silicon Investor.[5] Most users post their messages anonymously or more accurately, pseudononymously under fictional screen names.[6] This anonymity has fostered a robust and free-wheeling debate on Internet message boards. As in real speech, speech on the message boards and chat rooms includes true statements, valid insights, rank speculation, opinion, acerbic criticism, defamatory speech, trade secrets, irrational diatribe, and more.[7] Targets of online criticism cannot sue ISPs for failing to remove allegedly defamatory material, because section 230(c) of the *Communications Decency Act* grants ISPs broad immunity for such conduct.[8] That leaves only one defendant: John Doe.

Most cyberSLAPP cases involve statements on financial message boards or chat rooms.[9] Other possible arenas include Web sites where

4. *See generally* Matthew Helmer, *Brill's Content, The Money Press: Herd on the Net* <http://www.brillscontent.com/columns/moneypress_0599.html> (May 1999); Blake A. Bell, *Plaintiff Corporations Face Reprisals from Cybersmear Defendants*, 2 No. 4 e-Securities 1 (Dec. 1999).

5. *See generally* Helmer, *supra* n. 4; *see generally* Bell, *supra* n. 4.

6. *See generally* Helmer, *supra* n. 4.

7. *See* Greg Miller, *'John Doe' Suits Threaten Internet Users' Anonymity*, L.A. Times A1, ¶ 4 (Jun. 14, 1999). The concept of anonymous Internet postings has found its way into popular culture. *See The Simpsons*, "The Computer Wore Menace Shoes" (Fox Broad. Co. Nov. 26, 2000) (TV series). Homer posts scandalous and sometimes fictitious news on his Web site under the pseudonym "Mr. X," and surrenders his anonymity when he is awarded the Pulitzer Prize. *Id.*

8. 47 U.S.C. § 230(c) (1990) (stating that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); *Zeran v. Am. Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (stating that a failure to remove defamatory statements was an act shielded from liability by section 230(c)), *cert. denied*, 118 S. Ct. 2341 (1998).

9. *See generally* Jennifer Tanaka, *Beware What You Post*, Newsweek 90H (Oct. 30, 2000). A cottage industry has sprung up in which "cybersleuthing" companies monitor the Internet for unfavorable comments about their corporate clients. *Id.* Companies such as CyberScan, CyberAlert and eWatch monitor a variety of Internet sites, such as online news outlets, Usenet groups, Web logs and e-mail listserves. *See generally* Aparna Kumar, *Wired.com, Concern about New Web Monitors* <http://www.wired.com/news/print/

employees discuss the company they work for, or crudely named "sucks" Web sites posted by disgruntled customers or employees.[10] In the typical cyberSLAPP lawsuit, a company files suit against John Doe for posting an allegedly harmful message.[11] The company then tries to discover John Doe's identity by subpoenaing the message board host and John Doe's ISP.[12] Once the company learns John Doe's true identity, the company may simply drop the lawsuit and fire or otherwise sanction John Doe, if he works for the company.[13] Indeed, only rarely have companies litigated such claims to judgment.[14] Alternatively, the company may proceed with the lawsuit to deter this John Doe and future John Does

---

0,1294,41931,00.html> (Feb. 24, 2001). Two such services offer real-time monitoring, and one runs scans every fifteen minutes. *Id.* at ¶¶ 8–9.

10. Stephanie Armour, *USA Today, Employees Turn to Web for Gripes,* ¶¶ 1–3 <http://www.usatoday.com/life/cyber/tech/ctf572.htm> (Jul. 17, 1999); Mike France & Dan Carney, *Businessweek On-Line, Free Speech on the Net? Not Quite* ¶ 2 <http://www.businessweek.com:/2000/00_09/b3670155.htm?scriptFramed> (Feb. 28, 2000). An extremely brief Google search for "sucks" sites turned up www.mybosssucks.com, www.walmartsucks.com, www.chasebanksucks.com, www.etoys-sucks.com, www.homedepotsucks.com, www.survivorsucks.com, and many more. In the same vein are slightly more creative domain names like www.noamazon.com, www.starbucked.com, and www.pepsibloodbath.com (protesting Pepsi for advertising at bullfights). Such sites are not restricted to employment and commercial targets, as witnessed by three related sites, www.gwbushsucks.com, www.katherineharrissucks.com, and www.theelectoralcollegesucks.com. A New Jersey businessperson has amassed over 600 "sucks" domain names, all of which lead to his Sucks.com Web site. *See generally* Amy Standed, *Salon.com, The Saga of Sucks.com* <http://www.salon.com/tech/feature/2001/06/25/sucks/index1.html> (June 25, 2001). To readers who feel inspired to launch their own protest sites, I recommend Wired.com, Oscar S. Cisneros, *Wired.com, Legal Tips for Your 'Sucks' Site* <http://www.wired.com/news/politics/0,1283,38056,00.html> (Aug. 14, 2000).

11. Michael D. Goldhaber, *Associate Is a Leading 'Cybersmear' Lawyer,* N.Y.L.J. Law.Com <http://www.nylj.com/backpage/00/07/bp071400a2.html> (Jul. 14, 2000). Common claims against John Doe in cyberSLAPP suits include defamation, breach of fiduciary duty or duty of loyalty, tortious interference with business and contractual relations, misappropriation of trade secrets, misappropriation of identity of a corporate officer, breach of contract, unfair and deceptive trade practices, and securities fraud. Jay Eisenhofer & Sidney S. Liebesman, *Caught by the Net: What to Do If a Message Board Messes with Your Client* ¶ 18 <http://www.abanet.org/buslaw/blt/blt9-eisenhofer.html> (Sept./Oct. 2000).

12. *See generally* Goldhaber, *supra* n. 11.

13. *See e.g.* John Snell, *Prying into Posts,* Portland Oregonian B1 (Oct. 30, 2000) (discussing termination of formerly anonymous online posters by Raytheon and Answerthink).

14. *See* Bruce P. Smith, *Cybersmearing and the Problem of Anonymous Online Speech,* 18 Commun. Law. 3, at 3, 5 (Fall 2000). Boston attorney Carl Solomont is one of the handful of lawyers to obtain a judgment in a suit against John Doe. *Id.* The case, *Biomatrix v. Costanzo,* No. BER-L-670-00 (N.J. Super. Ct. Sept. 18, 2000) (on file with author), involved what the judge referred to as "extremely offensive and malicious" anonymous postings about officers of Biomatrix, including the claim that the officers were "Nazi doctors." Denise Magnell, *Fios, Inc., Libel Found on Internet Message Board Postings* <http://www.fiosinc.com/in_alm.html> (Aug. 4, 2000). After learning the posters' identity from Yahoo! and determining that two of the posters were Biomatrix employees, the plaintiffs obtained summary judgment on liability, leaving only a trial on damages. *See id.*

from posting similar comments.[15] John Doe often receives no notice of the lawsuit or the subpoena seeking his identity.[16] Even if John Doe receives advance notice, he may not be able to afford a lawyer to challenge the subpoena.[17]

II. THE COMPETING INTERESTS IN ANONYMITY AND ACCOUNTABILITY

Speakers choose anonymity for a variety of reasons. They may be "motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."[18] They may believe that their ideas will be more persuasive if their readers are unaware of their identity.[19] Of course, they may also be attempting to avoid blame for manipulating a stock price or defaming a company or person.[20]

The U.S. Supreme Court has long held that the First Amendment protects an author's right to remain anonymous. In 1960, in *Talley v. California*, the Court struck down a city ordinance prohibiting all anonymous leafleting because the fear of reprisal might deter "peaceful discussions of public matters of importance."[21] And in 1995, in *McIntyre v. Ohio Elections Commission*, the Court struck down a state law that prohibited the distribution of anonymous campaign literature, reasoning that "[a]nonymity is a shield from the tyranny of the majority."[22] Indeed, our nation's formative political debates over constitutional ratification took place beneath the cloak of anonymity, under such pseudonyms as Publius, Cato, and Brutus.[23]

The right to speak anonymously extends into cyberspace.[24] In 1997, a federal district judge relied on *McIntyre* to strike down a Georgia statute prohibiting the transmission of data on the Internet "if such data uses any individual name . . . to falsely identify the person."[25] The court rejected the state's claim that the statute applied only to individuals

15. *See* Eisenhofer, *supra* n. 11, at 46.

16. Carl S. Kaplan, N.Y. Times, *Cyberlaw Journal, Judge Says Online Critic Has No Right to Hide* <http://www.10.nytimes.com/library/tech/00/06/cyber/cyberlaw/09law.html> (June 9, 2000).

17. *Id.*

18. *McIntyre v. Ohio Elections Commun.*, 514 U.S. 334, 341-42 (1995).

19. *Id.* at 342.

20. *See infra* nn. 23-28 and accompanying text.

21. 362 U.S. 60, 64-65 (1960).

22. *McIntyre,* 514 U.S. at 342, 357.

23. *See id.* at 341-42. *See also NAACP v. Ala.*, 357 U.S. 449, 461 (1958) (vacating court order compelling disclosure of NAACP membership list because such an intrusion upon members' privacy would infringe their First Amendment freedom of association).

24. *See infra* n. 28 and accompanying text.

25. *Am. Civ. Liberties Union v. Miller*, 977 F. Supp. 1228, 1280 (N.D. Ga. 1997).

sending data with fraudulent intent or misappropriating another person's identity.[26] The court noted that the speaker's identity is part of the content of the speech and reasoned that the act would have a serious chilling effect on the many Internet users who use pseudonyms online.[27] Although preventing fraud was a compelling state interest, the statute was not narrowly tailored to serve that interest because it applied to both fraudulent and non-fraudulent speech.[28]

On the other hand, the right to speak anonymously is not boundless.[29] Unlawful anonymous postings can cause serious harm for which the authors should be held responsible. For example, a Pairgain Technologies employee posted a phony press release claiming that Pairgain had been taken over.[30] Pairgain's stock soared from $8.50 to $11.125 per share on the day he posted the release.[31] The employee pleaded guilty to securities fraud and was sentenced to five months home detention, five years probation, and $93,000 in restitution to investors who bought the stock and then sold at a loss after Pairgain debunked the false press release.[32] Similarly, an investor who had short-sold 3,000 shares of Emulex Corporation essentially betting that the price would fall circulated a fake news release stating that Emulex's chief executive officer had resigned and that Emulex planned to restate its earnings for the prior two years.[33] The stock price fell from $103 to $45 per share in an astonishing fifteen minutes.[34] The NASDAQ halted trading in the stock but not before the company lost over $2 billion in market valuation.[35] The perpetrator, who made a profit of around $240,000, later pleaded guilty to securities and wire fraud in exchange for federal prosecutors' recommendation that he be sentenced to 37 to 46 months in prison.[36]

---

26. *Id.* at 1232.

27. *Id.* at 1230, 1232.

28. *Id.*

29. *See infra* n. 32 and accompanying text.

30. Edward Wyatt, *Fake Web Posting Leads to Fraud Charge,* NY Times C1 (Apr. 16, 1999); Associated Press, *Pairgain Worker Sentenced in Fraud Case,* NY Times C1 (Aug. 31, 1999) [hereinafter *Pairgain Worker*].

31. Wyatt, *supra* n. 30, at C1; *Pairgain Worker, supra* n. 30, at C1.

32. Wyatt, *supra* n. 30, at C1; *Pairgain Worker, supra* n. 30, at C1.

33. Alex Berenson, *Guilty Plea Is Set in Internet Hoax Case Involving Emulex,* N.Y. Times C3 (Dec. 29, 2000) [hereinafter Berenson, *Guilty Plea*]; Alex Berenson, *On Hair-Trigger Wall Street, A Stock Plunges on Fake News,* N.Y. Times A1 (Aug. 26, 2000) [hereinafter Berenson, *On Hair-Trigger Wall Street*].

34. Berenson, *Guilty Plea, supra* n. 33, at C3; Berenson, *On Hair-Trigger Wall Street, supra* n. 33, at A1.

35. Berenson, *Guilty Plea, supra* n. 33, at C3; Berenson, *On Hair-Trigger Wall Street, supra* n. 33, at A1.

36. Berenson, *Guilty Plea, supra* n. 33, at C3; Berenson, *On Hair-Trigger Wall Street, supra* n. 33, at A1. Sentencing in the case was scheduled for August 2001. *See CBS Eve-*

Despite some valid claims, many legal experts and privacy advocates claim that companies are abusing the legal process simply to "out" their online critics.[37] Professor Lyrissa Barnett Lidsky notes that few cyberSLAPP plaintiffs expect their suits to end in a damages recovery.[38] Los Angeles attorney Megan Gray suggests that in "these cases, the (company) files the suits to find out the identity of John Doe. . . . They don't care about litigating against somebody with no money."[39] David Sobel of the Electronic Privacy Information Center agrees. "The companies don't care if they win. What they want are the names of their critics."[40] Public Citizen attorney Paul Levy suggests another motive for cyberSLAPP suits—to extract a humiliating apology, which both soothes the plaintiff's hurt feelings and deters future posters.[41]

Sometimes the fact that a company has learned John Doe's identity or filed a lawsuit will intimidate and deter John Doe and others from posting future messages.[42] A leading cyberSLAPP plaintiffs' lawyer suggests that "confessions by the perpetrators, as well as judgments against perpetrators will discourage others from similar postings on company boards."[43]

Learning John Doe's identity also allows the company to retaliate against John Doe, especially if John Doe is an employee. For example, Raytheon sued twenty-one John Does for alleged online disclosure of trade secrets.[44] After successfully subpoenaing their identities, Raytheon dropped the suit and fired four of the Does who were Raytheon employees.[45] A similar case of retaliatory termination ultimately led Yahoo! to change how it responded to John Doe subpoenas. A poster calling

---

ning News with Dan Rather, "Using the Internet to Commit Stock Fraud" (July 4, 2001) (tv broadcast).

37. Miller, *supra* n. 7, at A1.

38. Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 Duke L.J. 855, 876–77 (2000).

39. Howard Mintz, *'Cybersmear' Lawsuits Raise Privacy Concern*, Mercury News ¶ 20 <http://www0.mercurycenter.com/svtech/news/indepth/docs/boards112999.htm> (Nov. 28, 1999).

40. *See generally* Snell, *supra* n. 13.

41. E-mail from Paul Levy, Esq., to author (May 14, 2001) (copy on file with author).

42. Carl Solomont, *Scared Straight*, CIO Web Business 34, 36 <http://www.cio.com/archive/webbusiness/100199_gray_content.html> (Oct. 1, 1999) (noting that unmasking the poster or merely notifying the poster of the lawsuit can slow or stop the messages); Eisenhofer & Liebesman, *supra* n. 11, at 46 (stating that "[t]he mere filing of the John Doe action will probably slow the postings").

43. Bruce D. Fischman, *Your Corporate Reputation Online* ¶ 14 <http://www.fhdlaw.com/html/corporate_reputation.htm> (accessed Sept. 30, 2001).

44. Snell, *supra* n. 13.

45. *Id.* A Raytheon spokesman said of the employees' departure that they "voluntary quit." *Meet John Doe: Companies Target Online Chats*, Conn. Law Trib. ¶ 7 (Nov. 22, 1999).

himself Aquacool_2000 criticized AnswerThink Consulting Group on a Yahoo! message board.[46] AnswerThink subpoenaed Yahoo! to find out who Aquacool really was.[47] When it learned that he was an AnswerThink employee, AnswerThink fired him.[48] Los Angeles attorney Megan Gray filed suit on Aquacool's behalf against Yahoo!, claiming that Yahoo! violated Aquacool's privacy and its own privacy policy by disclosing Aquacool's information without notifying him.[49] Yahoo! settled the lawsuit and now provides notice to users before complying with John Doe subpoenas.[50]

III. EXISTING LAW DOES NOT ADEQUATELY PROTECT JOHN DOE'S ANONYMITY

Existing rules, statutes, and common-law doctrines are ill-suited to protecting John Doe's anonymity. Under existing procedures, John Doe sometimes receives no notice, and when he does, he may lack the time or money to retain counsel to challenge the subpoena.[51] Although some message board hosts and ISPs provide one or two weeks' notice, they are not required to give any notice and not all do.[52] Unless John Doe receives meaningful notice of the subpoena, cyberSLAPP plaintiffs will pierce John Doe's anonymity without any chance for judicial oversight.[53]

This section discusses the available strategies for either dismissing the complaint or forcing judicial review of the John Doe subpoena. Even the most promising of these strategies, a First Amendment challenge to the subpoena, does not guarantee notice or a hearing, nor does it guarantee that a court will examine the substantive merits of the plaintiff's claim.

---

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*; *Complaint, Doe v. Yahoo! Inc.* ¶ 1 (C.D. Cal. May 2000) (available at <http://legal.web.aol.com/decisions/dlpriv/aquacoolcomplaint.pdf>).

50. Greg Saitz, *Judge Affirms Privacy on the Net*, The Star Ledger ¶ 6 <http://www.nj.com/news/ledger/index.ssf?/jersey/ledger/119a548.html> (Nov. 20, 2000).

51. David L. Sobel, *The Process That "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 Va. J. L. & Tech. 3, at *14 (2000).

52. *Id.*; Miller, *supra* n. 7, at ¶ 24; Mintz, *supra* n. 39, at ¶ 12; Verne Kopytoff, *Online Speech Hit with Offline Lawsuits*, S.F. Chron. B1 (June 26, 2000).

53. *Doe v. 2TheMart.com*, 140 F. Supp. 2d 1088, 1095 n. 5 (W.D. Wash. 2001):

> This Court is aware that many civil subpoenas seeking the identifying information of Internet users may be complied with, and the identifying information disclosed, without notice to the Internet users themselves. This is because some Internet service providers do not notify their users when such a civil subpoena is received. The standard set forth in this Order may guide Internet service providers in determining whether to challenge specific subpoenas on behalf of their users. However, this will provide little solace to Internet users whose Internet service company does not provide them notice when a subpoena is received.

Id.

A. Personal Jurisdiction

If the plaintiff makes an unusual choice of forum, John Doe may challenge the court's personal jurisdiction over him.[54] For example, in *Melvin v. Doe*, the court dismissed a cyberSLAPP suit for lack of personal jurisdiction.[55] The only contact with the forum state of Virginia was America Online that based its business in Virginia and hosted the Web site in question on a Virginia server.[56] These contacts were insufficient to satisfy the Due Process Clause because John Doe's posting did not target any Virginia audience and concerned issues of local interest in Pennsylvania.[57] Personal jurisdiction, however, is not an especially useful tool for John Doe. Even if the court dismisses for lack of jurisdiction, the plaintiff can simply refile the action in another forum, as did the plaintiff in *Melvin v. Doe*.[58]

B. Anti-SLAPP Statutes

"SLAPP" is an acronym for strategic litigation against public participation.[59] In a typical SLAPP suit, a corporation files suit to intimidate a citizen who made critical statements to a governmental body about some issue that the company favors, such as a property development or business expansion.[60] Seventeen states[61] have enacted some form of "anti-

54. *Vail v. Doe*, 39 F. Supp. 2d 477, 477–78 (D. N.J. 1999). CyberSLAPP plaintiff attempting to sue in federal court may also face problems asserting diversity jurisdiction. *Id.* (alleging, upon information and belief, that John Doe was a citizen and resident of New York was insufficient to establish diversity jurisdiction).

55. 1999 WL 551335 (Va. Cir. Ct. June 24, 1999).

56. *Id.* at **1–2.

57. *Id.* at *2. The plaintiff in *Melvin*, a Pennsylvania judge, could have avoided jurisdictional problems by simply filing suit in Pennsylvania, where the plaintiff must have suspected the defendant lived or worked. Jonathan D. Silver, *Meeting Held to Breach Impasse Between Judge, Internet Writer*, Pitt. Post-Gazette D2 (Apr. 1, 2000). Perhaps the plaintiff, Judge Melvin, was leery of filing a defamation suit in Pennsylvania state court and likely further publicizing the allegedly defamatory statements. *Id.*

58. *Id.* For a discussion of the subsequent proceedings in *Melvin v. Doe*, in which the court ordered John Doe's identity disclosed, *see infra* § III.D.

59. Jerome I. Braun, *Increasing SLAPP Protection: Unburdening the Right of Petition in California*, 32 U.C. Davis L. Rev. 965, 969 (1999).

60. *Id*; Pring, *supra* n. 1, at 13–15.

61. Lori Potter, *Strategic Lawsuits Against Public Participation and Petition Clause Immunity*, 31 Envtl. L. Rep. 10852 n. 63 (July 2001) (noting that at least seventeen states have enacted some form of legislation to curb SLAPP suits). *See* Cal. Civ. Proc. Code § 425.16 (West Supp. 1997); Del. Code Ann. tit. 10, §§ 8136–8138 (Supp. 1996); Fla. Stat. Ann. § 768.295 (West 2000); Ga. Code Ann. § 9-11-11.1 (Supp. 1997); Ind. Code Ann. §§ 34-7-7-1–10 (West Supp. 1998); La. Code Civ. Proc. Ann. art. 971 (West 1999); Me. Rev. Stat. Ann. tit. 14, § 556 (West Supp. 1997); Mass. Gen. Laws Ann. ch. 231, § 59H (West 1997); Minn. Stat. Ann. §§ 554.01–05 (West Supp. 1997); Neb. Rev. Stat. §§ 25-21-241–246 (1995); Nev. Rev. Stat. 41.640–670 (Supp. 1993); N.Y. C.P.L.R. 3211(g) (McKinney 1997-1998); Okla. Stat. Ann. tit. 12, § 1443.1 (1999); 42 Pa. Cons. Stat. §§ 27-77-7707, 27-83-8301-8305

SLAPP" statute to deal with the disparity in resources between the typical parties to a SLAPP suit, and to diminish the threat that SLAPP suits pose to citizens' First Amendment right to petition the government.[62]

Some anti-SLAPP statutes require the SLAPP plaintiff to make a substantial evidentiary showing to avoid dismissal. For example, the California anti-SLAPP statute requires proof of a "reasonable probability that the plaintiff will prevail," and the Massachusetts statute requires proof that the defendant's exercise of her right to petition (1) was "devoid of any reasonable factual support or any arguable basis in law" and (2) injured the plaintiff.[63] This burden of production helps eliminate claims filed to intimidate citizens while still allowing legitimate claims to proceed.[64] Additionally, some anti-SLAPP statutes automatically stay discovery when the defendant invokes the statute.[65] Typical anti-SLAPP statutes provide for some combination of costs, legal fees and damages to be assessed against plaintiffs' whose suits are determined to violate the statute.[66]

In the hands of John Doe defendants, such tools would effectively balance anonymity and accountability by filtering out lawsuits filed simply to pierce John Doe's anonymity, while still allowing valid lawsuits to proceed. In *Global Telemedia International v. Doe*, the court relied on California's anti-SLAPP statute to dismiss a cyberSLAPP suit.[67] The court found that the plaintiff failed to show a reasonable probability of success because the John Does' statements were mere opinion, not fact, and because the plaintiff could show no correlation between online postings and falling stock prices.[68] After granting the Does' special motion to dismiss, the court awarded them $55,000 in attorneys' fees and costs under the anti-SLAPP statute.[69]

Most anti-SLAPP statutes, however, apply only where the defendant is sued for petitioning a governmental body, not for simply exercising the right of free speech.[70] Only California and Rhode Island's anti-SLAPP statutes protect the exercise of free speech more generally, though the

(2000); R.I. Gen. Laws §§ 9-33-1–4 (Supp. 1996); Tenn. Code Ann. §§ 4-21-1001–1003 (1997); Wash. Rev. Code Ann. §§ 4.24.500–520 (West Supp. 1997).

62. Braun, *supra* n. 59, at 969–70.

63. *E.g.* Cal. Civ. Proc. Code § 425.16(b)(1) (West 2001); Mass Gen. L. ch. 231, § 59H (West 1997).

64. Braun, *supra* n. 59, at 989.

65. *E.g.* Cal. Civ. Proc. Code § 425.16(g) (West 2001); Mass. Gen. L. ch. 231, § 59H (West 1997); R.I. Gen. L. § 9-33-2(b) (Supp. 1996).

66. Robert D. Sack, *Sack on Defamation* § 10.11.2, 10–65 (3d ed. P.L.I. 2000).

67. 132 F. Supp. 2d 1270, 1270–71 (C.D. Cal. 2001).

68. *Id.*

69. *Attorneys Report Winning $55,000 in Calif. Anti-SLAPP Law Litigation*, 18 Computer & Online Indus. Litig. Rep. 10 (Andrews Pubs., Inc., June 5, 2001).

70. Braun, *supra* n. 59, at 1036–40.

speech must pertain to issues of public concern.[71]

C. Motion to Dismiss and Motion to Stay Discovery

Where no anti-SLAPP statute is available, John Doe may try moving to dismiss the underlying complaint, and simultaneously moving to stay discovery pending resolution of the motion to dismiss. This, however, is a poor substitute for the automatic stay provision of an anti-SLAPP statute. The motion to dismiss itself places the cyberSLAPP plaintiff's claims under only minimal scrutiny. On a motion to dismiss, the question is merely whether accepting all well-pled facts as true and drawing every reasonable inference in the plaintiff's favor, the complaint states any valid claim for relief.[72] This standard is far more lenient that the evidentiary showing required under some anti-SLAPP statutes.[73]

John Doe may have some success moving to dismiss claims for defamation, the claim most commonly asserted against John Doe. In some states, the plaintiff must specify the allegedly defamatory statements in the complaint.[74] Pleading defamation with specificity often allows judges to dismiss complaints on the grounds that the statements are not defamatory[75] or that the statements are mere opinion or hyperbole.[76] Of course, John Doe still faces the logistical problem of finding counsel, preferably counsel familiar with the relatively specialized fields of defamation and Internet law.

D. First Amendment Challenge to the Subpoena

The First Amendment has proven to be a promising tool in several

---

71. Cal. Civ. Proc. Code § 425.16(e) (West 2001); R.I. Gen. L. § 9-33-2(a) (Supp. 1996). The court in *Global Telemedia Intl. v. Doe* held that comments on an Internet message board discussing a publicly traded company were statements on an issue of public concern under the California anti-SLAPP statute. 132 F. Supp. 2d at 1265–66. *Accord Hollis-Eden Pharm. v. AngelaWatch*, No. GIC 759462, slip op., 1–2 (Cal. Rptr. 2d Mar. 20, 2001) (copy on file with author) (stating that anonymous postings on a Yahoo! message board concerning plaintiff company was speech on a matter of public concern under California anti-SLAPP statute).

72. Charles A. Wright & Arthur R. Miller, Fed. Practice & Proc. 5A § 1357, text at nn. 36–39 (1990).

73. *See e.g.* Cal. Civ. Proc. Code § 425.16(b)(1) (West 2001) ("reasonable probability that the plaintiff will prevail on the claim"); Mass Gen. L. ch. 231, § 59H (2001) (proof that the defendant's exercise of its right to petition was "devoid of any reasonable factual support or any arguable basis in law" and resulting injury to the plaintiff).

74. Robert D. Sack, *Sack on Defamation* § 2.4.13 (3d ed. 2000). The court in *Dendrite Intl., Inc. v. Doe* required that a plaintiff seeking John Doe's identity must specify each allegedly wrongful posting, regardless of whether the claim is for defamation. *Dendrite Intl., Inc. v. Doe*, 2001 WL 770406, at *1 (N.J. Super. Ct. App. Div. July 11, 2001).

75. Lidsky, *supra* n. 38, at 873.

76. *See id.* at 919, 926.

recent John Doe cases.[77] In the first appellate decision to address the standard for reviewing a John Doe subpoena, *Dendrite International, Inc. v. Doe*,[78] the court relied on the First Amendment to grant John Doe substantial procedural and substantive protection.

1. *The* Dendrite *Standard*

Shortly after Dendrite filed a 1999 quarterly report with the SEC, a Yahoo! user calling himself "xxplrr" posted several comments about the company on a Yahoo! bulletin board devoted to discussing Dendrite.[79] The relevant comments asserted, in essence, that Dendrite manipulated its contracts and revenue-recognition policy to enhance subsequent years' earnings, and that Dendrite's president was trying to sell the company.[80]

Dendrite filed a defamation action against John Doe No. 3, a/k/a xxplrr,[81] and sought an order to show cause why Dendrite should not be granted leave to take limited discovery to learn John Doe's identity.[82] The trial court issued the order to show cause, and directed Dendrite to post the order on the Yahoo! Dendrite bulletin board.[83] However, the trial court denied Dendrite leave to take discovery because Dendrite failed to provide sufficient evidence that the messages caused Dendrite any harm.[84]

---

77. *See infra* n. 80 and accompanying text.

78. *Dendrite Intl.*, 2001 WL 770406.

79. *Id.* at *4.

80. *See id.* The full text of the challenged postings were as follows:

> John's [(Dendrite president John Bailye)] got his contracts salted away to buy another year of earnings and note how they're changing revenue-recognition accounting to help it.
>
> . . .
>
> Bailye has his established contracts structured to provide a nice escalation in revenue. And then he's been changing his revenue-recognition accounting to further boost his earnings (see about 100 posts back).
>
> . . .
>
> [Dendrite] signed multi-year deals with built-in escalation in their revenue year-over-year . . . .
>
> . . .
>
> [Dendrite] simply does not appear to be competitively moving forward. John [Bailye, Dendrite's president] knows it and is shopping hard. But Siebel and SAP already have turned him down . . . .

Id.

81. *Id.* at *5. In fact, Dendrite sued four John Does, but the appeal only involved John Doe No. 3, a/k/a/ xxplrr. *Id.* Only John Does Nos. 3 and 4 appeared to oppose Dendrite's motion for leave to take discovery. *Dendrite Intl., Inc. v. Does*, No. MRS C-129-00, slip op. at 5 (copy on file with author).

82. *Dendrite Intl.*, 2001 WL 770406, at *5.

83. *Id.*

84. *Dendrite Intl.*, No. MRS C-129-00, slip op. at 12–13 (copy on file with author). Dendrite offered evidence that on each day that one of the Does posted one of the messages

On appeal, the Appellate Division of the New Jersey Superior Court established a detailed framework to "strike[ ] a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation . . . ."[85] First, plaintiffs must attempt to notify John Doe of the subpoena or application by posting notice on the message board, and judges should allow John Doe a reasonable time to oppose the application.[86] Plaintiffs must also "identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech."[87]

Next, plaintiffs must produce evidence to support each element of their claim. "In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim . . ., the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie case basis . . . ."[88] Finally, if plaintiffs make the requisite evidentiary showing, "the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."[89]

Applying the prima facie evidence standard, the appellate division held that Dendrite had not produced sufficient evidence that John Does' statements caused Dendrite any cognizable harm.[90] The record did not support the conclusion that John Does' postings impaired Dendrite's

---

sued upon, Dendrite's stock value dropped by between three percent and eleven percent. *Id.* The court noted, however, that Dendrite's stock value also dropped on days that the Does did not post messages and rejected Dendrite's claim of a causal link between the postings and decreases in its stock price. *Id.* The trial court also held that Dendrite had not established its claim for misappropriation of trade secrets because John Does Nos. 3 and 4 certified that they were not Dendrite employees. *Id.* at 16–17.

85. *Dendrite Intl.*, 2001 WL 770406, at *1.

86. *Id.*

87. *Id.*

88. *Id.* Much of the opinion was spent clarifying the standard that the trial court applied. *Id.* The trial court purported to examine whether the complaint could survive a motion to dismiss for failure to state a claim. *Dendrite Intl.*, No. MRS C-129-00, slip op. at 9. In fact, the court looked beyond the face of the complaint and considered whether, on the certifications and documentary evidence submitted, Dendrite would likely prevail on each element of its claims. *Id.* at 4, 12–13. The court, however, did not require proof of actual malice because Dendrite could not be expected to establish actual malice without learning the Does' identities. *Id.* at 15.

89. *Id.* at *2. Because the plaintiff failed to satisfy the prima facie evidence threshold, the court did not balance the strength of the prima facie case and the need for disclosure against the interest in anonymity. *See id.* at **13–14.

90. *Id.*

stock value,[91] and Dendrite offered no evidence to support its allegation that the postings would inhibit its hiring practices.[92] The court, therefore, affirmed the trial judge's conclusion that Dendrite failed to show a sufficient nexus between the postings and Dendrite's alleged harm.[93]

The court applied a similarly restrictive standard in *Doe v. 2TheMart.com*,[94] though the court noted that the standard applied to cases in which John Doe was not a party.[95] 2TheMart.com ("TMRT") was defending a shareholder derivative suit alleging fraud on the market.[96] Among TMRT's numerous affirmative defenses was the claim that no act or omission by TMRT's officers and directors caused the plaintiffs' injury, i.e., the decline in TMRT's stock price.[97] TMRT had been the subject of discussion on an Internet message board hosted by Silicon Investor.[98] Several anonymous users, calling themselves "Truthseeker" and "Cuemaster," posted messages asserting serious wrongdoing by TMRT and its chief executive officer.[99]

TMRT subpoenaed Silicon Investor, seeking the identities of twenty-three users who either posted messages on the board *or* communicated via the Internet with users who posted messages.[100] InfoSpace, which operated the Silicon Investor Web site, gave notice of the subpoena to these users, and a user called "NoGuano" filed a motion to quash the subpoena.[101]

The court noted the First Amendment interest in anonymous speech, and reasoned that that interest deserves even greater protection

91. *Id.* NASDAQ trading records showed that Dendrite's stock lost value on three of the days immediately following postings but gained value on five of the days immediately following a posting. Over those days, Dendrite's stock gained 3 5/8 points. *Id.* at *14.

92. *Id.*

93. *Id.* One court applied a test that while vague, may be more restrictive than the *Dendrite* test. *See Varian v. Delfino*, No. CV 780187 (Cal. Rptr. 2d Mar. 7, 2001) (available at<http://www.geocities.com/SiliconValley/Hardware/8784/slapp/cabrinhaord.html?>). In a one-paragraph order, the California Superior Court quashed a subpoena seeking the identity of several non-party John Does. *Id.* The court held that John Doe's constitutional right to free speech and privacy allowed him to express himself anonymously in a public forum, like the Internet, unless the subpoenaing party showed a "compelling need" for John Doe's identity. *Id.*

94. 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

95. *Id.* at 1095.

96. *Id.* at 1089.

97. *Id.* at 1090.

98. *Id.*

99. *Id.* One message read: "TMRT is a Ponzi scam that Charles Ponzi would be proud of. . . . The company's CEO, Magliarditi, has defrauded employees in the past. The company's other large shareholder, Rebeil, defrauded customers in the past." Another claimed that TMRT was "dumped by their accountants . . . these guys are friggin liars . . . why haven't they told the public this yet??? Liars and criminals!!!!!" *Id.*

100. *Id.* at 1090.

101. *Id.* at 1091.

when John Doe is not a party to the underlying lawsuit.[102] The court announced four factors to be balanced when reviewing such nonparty John Doe subpoenas: (1) whether the subpoena "was issued in good faith and not for any improper purpose"; (2) whether the information sought relates to a core claim or defense"; (3) whether the information "is directly and materially relevant to that claim or defense"; and (4) whether "information sufficient to establish or disprove that claim or defense is available from any other source."[103]

The court found that the breadth of the subpoena was suggestive of bad faith, though the court stopped short of actually finding bad faith.[104] The court further found that the affirmative defense to which TMRT claimed the information was relevant—that no act or omission by the officers or directors caused plaintiffs' harm—was not a "core" defense.[105] Other defenses such as the absence of material misstatement or disclosure of material facts by the defendants went more to the "heart of the matter."[106] Finally, the anonymous posters' identities were not "directly and materially relevant" to the causation defense because if the postings did diminish the stock price, they did so without anyone knowing the speakers' identities.[107]

2. *Less Protective Standards*

Several other courts, however, have developed less protective First Amendment standards that ask only whether the plaintiff's claim would survive a motion to dismiss for failure to state a claim. Unlike *Dendrite*, neither of these courts imposed any notice requirement.

In *Melvin v. Doe*,[108] the Pennsylvania Court of Common Pleas allowed the plaintiff to discover John Doe's identity. Plaintiff sued John Doe for making allegedly defamatory statements about her on an America Online message board. The court ordered John Doe's identity disclosed, although it limited that disclosure at least until the trial to the plaintiff and her counsel.[109]

---

102. *Id.* at 1095.

103. *Id.*

104. *Id.* at 1095–96. The subpoena sought "[a]ll identifying information and documents, including, but not limited to, computerized or computer stored records and logs, electronic mail (E-mail), and postings on your online message boards," concerning a list of twenty-three Infospace users. *Id.* at 1090 n. 1. In response to the court's concern over the subpoena's breadth, TMRT's counsel stated that TMRT sought only the identity of the twenty-three listed users. *Id.*

105. *Id.* at 1096.

106. *Id.*

107. *Id.* at 1097.

108. No. GD99-10264, slip op. (Pa. Ct. Cm. Pl. Nov. 15, 2000) (copy on file with author).

109. *Id.* at 30–31.

The court adopted a two-prong test to determine when a plaintiff may discover John Doe's identity. First, "the complaint on its face [must] set forth a valid cause of action."[110] And second, "the plaintiff [must] offer testimony that will permit a jury to award damages."[111] The court recognized that this threshold "can be easily met" because the plaintiff need only (1) demonstrate that the statements appeared on the Internet and, if false, would support a defamation recovery, and (2) testify that the statements are false "and that she has experienced emotional distress as the result of the statements."[112] The second prong of the test adds nothing to the first. The plaintiff need only file an affidavit averring that the statements are false and that she experienced emotional distress. The court did not explain what evidence the plaintiff supplied to satisfy the test, although the court did note that it was simultaneously denying John Doe's motion for summary judgment "because plaintiff has produced evidence which would support a finding that the statement was made, the statement was false, the statement was defamatory, and she has sustained actual harm."[113]

The court's rationale for fashioning such a lenient test rests on the false choice that the court posited. Recognizing the competing interests in anonymity and accountability, the court claimed that there were only two possible resolutions of that conflict: (1) that the First Amendment provides an absolute privilege for anonymous speakers, in which case state law could not protect against anonymous but tortious speech; and (2) that John Doe will lose his anonymity even though a jury may later find that the statements were true or otherwise not actionable.[114] This short sighted approach ignores the possibility of a middle ground between these two extreme possibilities, which the *Dendrite* court achieved.

In the case *In re America Online*,[115] a Virginia court also used what

110. *Id.* at 14.

111. *Id.* The *Melvin* court spoke inconsistently about the standard it was applying. *See id.* At the beginning of its opinion, the court initially stayed discovery of John Doe's identity until "the Doe defendants had an opportunity to establish that, as a matter of law, plaintiff could not prevail in the lawsuit." *Id.* at 2. This, of course, differs from the test the court ultimately applied that required the plaintiff to produce evidence to support its claims, though it required only a bare minimum of evidence.

112. *Id.* at 14. The court based its standard on rule 4011(b) of the Pennsylvania Rules of Civil Procedure, which prohibits discovery that would cause unreasonable annoyance, embarrassment, oppression, burden, or expense to any person or party. *Id.* at 2, n. 2. Based on rule 4011(b), the court held that "[a] plaintiff should not be able to use the rules of discovery to obtain the identity of an anonymous publisher simply by filing a complaint that may, on its face, be without merit." *Id.*

113. *Melvin v. Doe*, No. GD99-10264, 3 slip op. (Pa. Ct. Cm. Pl. Nov. 15, 2000).

114. *Id.* at 20.

115. No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds*, 542 S.E.2d 377 (Va. 2001) [hereinafter *In re AOL*]. Both parties in the case valued their

amounted to a motion-to-dismiss standard to balance the interests in anonymity and accountability, though it purported to apply a different standard. In the *AOL* case, AOL itself moved to quash the subpoena to identify the John Doe defendants in an Illinois action.[116] The court stated that it would not order disclosure unless it was "satisfied by the pleadings or evidence supplied to the court" that (1) "the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where the suit was filed" and (2) "the subpoenaed identity information is centrally needed to advance that claim."[117]

The court summarily stated that the pleadings and the Internet postings satisfied the test but did not describe the pleadings or postings, probably because disclosing the postings might have harmed the plaintiff's stock price.[118] That finding sheds little light on how stringent the "good faith basis" standard is. The court may be satisfied by "the pleadings or evidence supplied" which suggests that the plaintiff could meet the standard on the pleadings alone, perhaps by simply pleading a prima facie case.[119] Additionally, the court rejected as "unduly cumbersome" AOL's proposal that plaintiff "must have pled with specificity a prima facie claim."[120] So, apparently, one can show a "legitimate, good faith basis to contend that it may be the victim of" actionable conduct by something less than pleading with specificity a prima facie claim.[121] Perhaps the court's standard allows for mere notice pleading that might not satisfy AOL's proposal to be supplemented by additional evidence. In any case, the court's standard is more lenient than that adopted in *Dendrite*.

Though case-by-case First Amendment challenges have proven to be John Doe's most successful strategy to date, this approach has its shortcomings. First, as we have already seen, the case-by-case approach may lead to inconsistent levels of protection, with some courts applying relatively toothless standards of review. One case to date even rejected out-

---

anonymity. *See Am. Online, Inc. v. Anonymous Publicly Traded Co.*, 2001 WL 1210372, at *1 n. 6. The plaintiff called itself "Anonymous Publicly Traded Company," or "APTC," apparently to avoid publicizing statements that it felt could lower its stock price. *See id.* The plaintiff redacted its name from copies of the postings supplied to AOL's counsel and filed unredacted copies under seal. *Id.* The Virginia Supreme Court did not address the appropriate standard for review of the John Doe subpoena. *In re AOL*, 542 S.E.2d at 354–55. Instead, it held that the lower court abused its discretion by allowing the plaintiff to proceed anonymously. *Id.*

116. *In re AOL*, 2000 WL 1210372, at *1.

117. *Id.* at *8.

118. *Id.*

119. *Id.*

120. *Id.* at *7. AOL also proposed a second element which the court adopted: that the identity be centrally needed to advance the claim. *Id.*

121. *Id.* at **7–8.

right the notion that John Doe's anonymous speech merited any protection.[122] Second, the case-by-case approach may not adequately address John Doe's need for notice and a hearing before the ISP discloses his identity. The following two sections discuss a proposed amendment to ECPA that would provide uniform notice and hearing requirements and standards of review.

IV. AMENDING ECPA TO GUARANTEE JOHN DOE MEANINGFUL NOTICE AND THE OPPORTUNITY FOR A HEARING

The strategies listed in the previous section are irrelevant unless John Doe receives meaningful notice that his ISP has received a subpoena. This article proposes an amendment to ECPA[123] prohibiting the disclosure of John Doe's identity unless the plaintiff gives John Doe reasonable notice and obtains a court order authorizing the disclosure.[124] The plaintiff could satisfy the notice requirement by posting a link to electronic versions of the pleadings and motion papers on the message board where the allegedly wrongful statements occurred, and e-mailing the same documents to all known addresses for John Doe.[125]

Piercing John Doe's anonymity without notice or the opportunity to challenge subpoena violates our most basic notions of procedural due process. "The core of due process is the right to notice and a meaningful opportunity to be heard."[126] The Fifth and Fourteenth Amendments prohibit government from depriving citizens of life, liberty or property without due process of law.[127] The exercise of First Amendment rights constitutes a protected liberty interest that the government may not

122. *Message Board Posters Have No Right to Anonymity, Florida Appeals Court Rules*, Mealy's Cyber Tech Litig. Rep. (Nov. 2000) (discussing *Hvide v. Doe*). The trial court did not issue a written opinion. *Id.* The Third District Court of Appeal denied John Doe's certiorari petition, and did not address the merits of John Doe's First Amendment argument. *See id.; Does v. Hvide*, No. 3D00-1693 (Fla. Dist. Ct. App. Oct. 12, 2000) (copy on file with author) (denying certiorari and dissolving stay pending appeal).

123. 18 U.S.C. § 2703 (c)(1)(A) (2001) (stating that ISPs may disclose when subpoenaed by a person other than a governmental agency).

124. *See* the Appendix to this Article for the text of the proposed amendment. David Sobel has also proposed amending ECPA to require "presentation of a subpoena before information identifying an Internet user can be disclosed to any party" and that "upon receipt of a civil subpoena for information concerning a subscriber or user, a service provider must notify the individual of the request. *See* Sobel, *supra* n. 51, at **19–20. "A reasonable amount of time should be allowed for the individual to take appropriate action, e.g., move to quash, before any identifying information is disclosed." *Id.*

125. The amendment also prohibits the plaintiff from attempting to use this notice procedure to learn John Doe's identity.

126. *LaChance v. Erickson*, 522 U.S. 262, 266 (1998).

127. U.S. Const. amend. V; *id.* at amend. XIV, § 1.

deny without due process.[128] Courts in a variety of contexts have held that judicial orders enforcing discovery requests constitute state action.[129]

The familiar balancing test of *Mathews v. Eldridge*[130] governs the extent of procedural protection that John Doe is due. One side of the balancing test weighs both the private interest implicated and the risk of an erroneous deprivation through existing procedures.[131] The other side weighs the government's interest in not providing further procedures.[132]

---

128. *See e.g. Procunier v. Martinez*, 416 U.S. 396, 418 (1974) (invalidating the prison policy of censoring inmates' mail because "[t]he interest of prisoners and their correspondents in uncensored communication by letter, grounded as it is in the First Amendment, is plainly a 'liberty' interest within the meaning of the Fourteenth Amendment even though qualified of necessity by the circumstance of imprisonment. As such, it is protected from arbitrary governmental invasion."), *overruled on other grounds by Thornburgh v. Abbott*, 490 U.S. 401 (1989) (overruling *Procunier*'s standard of review for incoming mail but not outgoing mail); *NAACP*, 357 U.S. at 460 (stating that "freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech").

129. *See id.* at 461 (compelling production of NAACP membership records violated First Amendment freedom of association); *Grandbouche v. Clancy*, 825 F.2d 1463, 1466 (10th Cir. 1987) (enforcing private party's discovery request which sought membership list of organization espousing "dissident views on the federal income tax system," stating it constituted state action and implicated First Amendment freedom of association); *Britt v. Superior Court*, 574 P.2d 766 (Cal. 1978) (stating that the First Amendment freedom of association prohibited enforcement of discovery request demanding names of all persons, including non-litigants, who attended meetings of groups opposed to airport noise); *Snedigar v. Hoddersen*, 786 P.2d 781 (Wash. 1990) (remanding for consideration of whether private subpoena seeking political association's meeting minutes violated First Amendment associational privilege); *L.A. Meml. Coliseum v. Natl. Football League*, 89 F.R.D. 489 (C.D. Cal. 1981) (applying First Amendment reporter's privilege to quash subpoena seeking identity of journalist's confidential sources).

A recent case quashing a cyberSLAPP plaintiff's subpoena seeking John Doe's identity recognized that enforcement of the subpoena would have constituted state action. *See 2TheMart.Com*, 140 F. Supp. 2d at 1091–92 (stating that the First Amendment freedom of speech prohibited enforcement of subpoena seeking John Doe's identity). The foregoing state action determinations are logical extensions of the Supreme Court's holding that "the application of state rules of law in state courts in a manner alleged to restrict First Amendment freedoms constitutes "state action" under the Fourteenth Amendment." *Cohen v. Cowles Media Co.*, 501 U.S. 663, 668 (1991) (stating that judicial enforcement of "promissory estoppel, a state-law doctrine which, in the absence of a contract, creates obligations never explicitly assumed by the parties . . . is enough to constitute "state action" for purposes of the Fourteenth Amendment"); *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964) (stating that judicial application of state defamation law in action between private parties constituted sufficient state action to trigger of First and Fourteenth Amendment protections). *See also Shelley v. Kraemer*, 334 U.S. 1, 19 (1948) (holding that judicial enforcement of racially discriminatory restrictive covenants constitutes sufficient state action for purposes of Fourteenth Amendment equal protection claim).

130. 424 U.S. 319 (1976).

131. *Id.* at 335.

132. *Id.*

Application of this test weighs heavily in favor of affording John Doe notice and the opportunity for a hearing.

John Doe's pan of the scale is brim full. As discussed above, the Supreme Court has recognized the importance of anonymous speech, both historically and in contemporary society.[133] Additionally, the existing procedures, or lack thereof, carry a serious risk of erroneous deprivation. The risk that plaintiffs may abuse the unsupervised exercise of civil subpoena power is evidenced not only in anecdotal accounts of abuse[134] but also in John Doe's success rate in cases where courts have actually reviewed the subpoena.[135] Indeed, even the mere appearance of counsel for John Doe often prompts cyberSLAPP plaintiffs to settle the lawsuit.[136]

In contrast, states have little reason to oppose further procedural protections. In fact, the rules in most jurisdictions contemplate notice and a hearing, though not all cyberSLAPP plaintiffs follow those rules to the letter. For example, most jurisdictions prohibit plaintiffs from taking depositions until twenty to thirty days after service of the summons and complaint, except with leave of court.[137] However, when cyber-

133. *See McIntyre v. Ohio Elect. Commn.*, 514 U.S. 334, 341–42 (1995); *see also NAACP*, 357 U.S. at 461.

134. *See supra* § II.

135. In the John Doe cases cited in this article, four courts have refused to order disclosure of John Doe's identity, three have done so only after reviewing either the prima facie evidence or at least the complaint, and one has rejected any special First Amendment protection. *See Dendrite Intl.*, 2001 WL 770406 (refusing to order disclosure); *2TheMart.com*, 140 F. Supp. 2d 1088 (refusing to order disclosure); *Hollis-Eden Pharm.*, No. GIC 759462, slip op. at 1–2 (refusing to order disclosure); *Varian*, No. CV 780187 (refusing to order disclosure); *Immunomedics*, No. A-2762-00T1, 2001 WL 770389 (ordering disclosure after review of prima facie evidence and balancing of interests); *In re AOL*, No. 40570, 2000 WL 1210372 (ordering disclosure after reviewing complaint and Internet postings); *Melvin*, No. GD99-10264, slip op. (ordering disclosure after reviewing complaint and requiring "testimony that will permit a jury to award damages"); *Hvide* (as discussed in *Message Board Posters Have No Right to Anonymity, Florida Appeals Court Rules*, Mealy's Cyber Tech Litig. Rep., Nov. 2000 (finding no First Amendment protection), *appeal dismissed*, Order, No. 3D00-1693 (Fla. Dist. Ct. App. Oct. 12, 2000) (copy on file with author)). *See also Global Telemedia* (dismissing complaint under California's anti-SLAPP statute).

136. *See e.g. Case Against Doe Defendants Dropped by Plaintiffs*, Mealy's Cyber Tech Litig. Rep. (Mar. 2001); Electronic Frontier Foundation, *Press Release: Medinex Drops Suit Against Anonymous Online Critics* ¶ 1 <http://www.eff.org/Legal/Cases/Medinex_v._Awe2bad4mdnx/20010522_eff_dismiss_pr.html> (May 22, 2001).

137. *See e.g.* Ala. R. Civ. P. 30(a) (2001) (imposing a thirty-day prohibition); Alaska R. Civ. P. 26(d)(2)(A) & 30(a)(2)(C) (2001) (imposing a thirty-day prohibition); Ariz. R. Civ. P. 30(a) (2001) (imposing a thirty-day prohibition); Mass. R. Civ. P. 30(a) (2001) (imposing a thirty-day prohibition). Until the 1993 amendments, Fed. R. Civ. P. 30(a) imposed the same thirty-day prohibition. *See* Fed. R. Civ. P. 30, Advisory Committee Notes to 1970 Amendments, subdivision (a). Today, federal rules require leave of court for discovery prior to the mandatory Rule 26(f) conference, which obviously cannot occur if the plaintiff does not know John Doe's identity. Fed. R. Civ. P. 30(a)(2)(C) (2001).

SLAPP plaintiffs do seek leave to serve expedited discovery, many do not make the court aware of the potential harm to John Doe's First Amendment rights, and busy courts often rubber stamp plaintiffs' requests.[138] Additionally, most rules of civil procedure require notice of any subpoena to be served on all parties.[139]

To address these procedural failings, this article proposes a notice and hearing requirement modeled after the *Video Privacy Protection Act of 1988* (the "VPPA").[140] The VPPA prevents video stores from disclosing information about the movies a consumer has rented in response to mere civil subpoenas.[141] Instead, a party seeking the information must obtain a court order upon a showing of a "compelling need for information unavailable through any other means" and give the consumer reasonable notice of the court proceeding.[142] The case for notice is far more compelling for John Doe who is threatened not simply with the unwarranted disclosure of information about video rental habits, but infringement of his First Amendment right to speak anonymously. For that reason, the *Dendrite* court declared that John Doe is entitled to notice and an opportunity to be heard before a court orders disclosure.[143]

Notice is futile if it does not afford John Doe a reasonable opportunity to find counsel and challenge the subpoena. John Doe may not have sufficient time or information to find an attorney.[144] Time to find counsel is especially critical for John Doe, since representing himself is effectively impossible without sacrificing his anonymity. To enter an appearance, John Doe would have to give the clerk's office a name and

138. *See* E-mail from Megan Gray, Esq., to author (May 21, 2001) (copy on file with author).

139. *See e.g.* Fed. R. Civ. P. 26(b)(1) (2001) (stating that party taking oral deposition must give reasonable notice to every other party); Fed. R. Civ. P. 45(b)(1) (2001) (stating that the subpoenaing party must serve on all other parties prior notice of documents and things to be produced); Mass. R. Civ. P. 30(b)(1) (2001) (stating that the party taking oral deposition must give reasonable notice to every other party); Mass. R. Civ. P. 45(d)(1) (2001) (requiring that no deposition subpoena shall issue prior to service of notice).

140. *See* 18 U.S.C. § 2710(b)(2)(F) (2001). Congress passed the VPPA in the wake of the controversial confirmation hearings on Judge Robert Bork's Supreme Court nomination, when a Washington, D.C. newspaper reporter obtained a printout of the movies Judge Bork rented from his neighborhood video store. *See* Simson Garfinkel, *Database Nation*, 72 (O'Reilly, 2000). Though many remember the controversy over the reporter obtaining the rental records in the hope of demonstrating that he rented pornographic films, fewer remember that the records revealed nothing controversial. As it turned out, most of the 146 movies were Disney movies and Hitchcock films. *See id.*

141. 18 U.S.C. § 2710(b)(2)(F) (2001).

142. *Id.*

143. *See Dendrite Intl.*, No. A-2774-00T3, 2001 WL 770406, at *1.

144. *See generally* John Does Anonymous Foundation <http://www.johndoes.org> (accessed Oct. 24, 2001). For a John Doe who learns he is the target of a subpoena, a good resource for information and contacts is the Web site of the John Does Anonymous Foundation. *Id.*

address for sending notices and orders. Merely attending a hearing would give away John Doe's identity if the plaintiff's representative would recognize him.[145] On the other hand, the cyberSLAPP plaintiff will not be prejudiced by giving John Doe time to find counsel. CyberSLAPP claimants rarely seek preliminary injunctions, and even if they did, such an order would almost certainly constitute an invalid prior restraint.[146] This article, therefore, proposes a thirty-day notice period during which the ISP is prohibited from complying with the subpoena.

Finally, the notice should be accompanied by all relevant papers, including the subpoena, the underlying complaint, and the motion papers seeking the disclosure order, so that John Doe has sufficient information to challenge the subpoena. The plaintiff should post the notice in the message board or chat room where John Doe posted his allegedly wrongful comments, perhaps with a link available from which John Doe could download the documents.[147] Additionally, the plaintiff should e-mail the notice to all known e-mail addresses for John Doe.[148]

The proposed notice and hearing requirement mitigates the shortcomings of the existing system. And even if John Doe never receives the notice,[149] cannot find a lawyer, or is intimidated at the thought of a legal battle, the required hearing still guarantees a measure of judicial oversight. The following section discusses the finding that courts should make before ordering disclosure of John Doe's identity.

---

145. David Sobel has proposed that courts "establish procedures whereby an anonymous defendant could submit *pro se* written objections to a subpoena without disclosing his or her identity to opposing counsel." Sobel, *supra* n. 51, at *21. Paul Levy suggests the possibility of establishing an anonymous e-mail address to which the court and other parties could address notices and orders. E-mail from Paul Levy, Esq., to author (May 14, 2001) (copy on file with author). I thank Paul Levy for pointing out the logistical implausibility of preserving one's anonymity while acting *pro se*.

146. *See* Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 Duke L.J. 147 176 (1998) (prior restraint doctrine embodies a judgment that even a preliminary injunction against speech that will probably be found libelous poses too great a burden on free speech rights). Courts will invalidate nearly any preliminary injunction in a defamation case as an unconstitutional prior restraint. *Id.*

147. The statute would have to prohibit the cyberSLAPP plaintiff from trying to trace John Doe's identity when he downloads the documents.

148. With some ISPs, John Doe's e-mail address is a combination of the screen name or pseudonym by which he identifies his posts, combined with the ISP's domain name for example, aquacool_2000@yahoo.com. Other online services allow John Doe to include an e-mail address in a profile available to other users.

149. He may have stopped using the message board and e-mail address to which the notice is sent.

V. AMENDING ECPA TO GUARANTEE JUDICIAL SCRUTINY AND PREVENT NEEDLESS INTRUSION ON JOHN DOE'S ANONYMITY

Though cyberSLAPP claims against John Doe are a recent invention, there are well-established judicial approaches for balancing First Amendment interests and accountability interests in other contexts. This section discusses two familiar approaches and considers the guidance that each holds for courts reviewing John Doe subpoenas.

A. REPORTER'S PRIVILEGE

The approach most analogous to reviewing of a John Doe subpoena is the reporter's privilege, a qualified privilege against compelled disclosure of reporters' confidential sources.[150] The principles underlying the reporter's privilege are quite simple. If reporters could not promise their sources confidentiality, they would find it impossible to discover and report important news stories.[151] This First Amendment interest in the free flow of information, however, can conflict with a litigant's interest in discovering evidence necessary to prove her case.[152] Although the specific formulations of the privilege vary slightly, they serve the same core function: to balance the need for disclosure and the need for confidentiality by testing the subpoenaing party's claim.[153]

The existing reporter's privilege formulations involve varying degrees of scrutiny of the underlying complaint. Most courts require that the information sought must be: (1) highly material and relevant to the underlying claim, (2) necessary or critical to maintenance of the claim, and (3) unavailable from alternative sources.[154] To avoid needless intrusion on anonymity, many courts also delve into the merits of the plaintiff's claims and refuse to order disclosure unless plaintiff has a viable claim.[155] Other courts, however, consider only whether the litigant has pleaded a prima facie case and do not require evidence to support the claim.[156]

---

150. Courts have extended the privilege beyond traditional news reporters to include authors and academics. *See e.g. In re Cusumano*, 162 F.3d 708 (1st Cir. 1998) (academic researchers and commentators); *Shoen v. Shoen*, 5 F.3d 1289 (9th Cir. 1993) (author of an investigative book); *Silkwood v. Kerr-McGee*, 563 F.2d 433 (10th Cir. 1977) (documentary filmmaker).

151. *See Bruno & Stillman, Inc. v. Globe Newsp. Co.*, 633 F.2d 583 (1st Cir. 1980).

152. *See id.*

153. *See id.* at 597–98.

154. *See* 23 Wright & Miller, Fed. Practice & Proc. § 5426, at 789.

155. *See Zerilli v. Smith*, 656 F.2d 705 (D.C. Cir. 1981); *Bruno & Stillman*, 633 F.2d at 597; *Natl. Union Fire Ins. Co. v. Seafirst Corp.*, 14 Med. L. Rep. 1190 (W.D. Wash. 1987).

156. *See In re Selcraig*, 705 F.2d 789 (5th Cir. 1983); *Rogers v. Home Shopping Network*, No. CV 98-6326 DDP (BQRx), 28 Med. L. Rptr. 1107 (C.D. Cal. Oct. 15, 1999); *Dangerfield*

The flexible balancing approach of the reporter's privilege cases is well suited to reviewing John Doe subpoenas. First, those courts that examine the substantive merits of the underlying claim can assess the weight of the interest in accountability, and therefore decide when there is a sufficiently compelling interest to justify intruding on the confidential relationship between reporter and source. Second, the reporter's privilege standard allows courts to distinguish between cases where the anonymous source's identity is essential to the case, e.g., where the source relied upon might help prove that a reporter acted with actual malice, from cases where the anonymous source's identity has little bearing on any claim. The latter cases present a far less weighty interest in disclosure than the former.

Both of these nuances are particularly important for evaluating the balance between anonymity and accountability in John Doe cases. First, courts must review the substantive merits of the cyberSLAPP plaintiff's claim to evaluate the interest in accountability. Second, a requirement that John Doe's identity be directly relevant helps prevent disclosure where a litigant has a valid claim, but disclosing John Doe's identity would do little, if anything, to advance that claim. This might be the case where John Doe is not the defendant, and his identity is only marginally relevant, if at all.[157]

---

v. Star Editorial, Inc., 817 F. Supp. 833 (C.D. Cal.), *mandamus denied*, 7 F.3d 856 (9th Cir. 1993); *Mitchell v. Superior Court*, 690 P.2d 625 (Cal. 1984).

Courts have imported the reporter's privilege approach to review discovery requests that threaten the First Amendment freedom of association. *See e.g. Sneidigar v. Hoddersen*, 786 P.2d 781, 783–84 (Wash. 1990) (remanding order compelling production of fringe political group's meeting minutes so that trial court could determine whether plaintiff had shown requisite relevancy of information sought and lack of alternative sources and could balance need for information against need for nondisclosure); *Black Panther Party v. Smith*, 661 F.2d 1243, 1268 (D.C. Cir. 1981) (reversing order dismissing claim as sanction for failure to answer interrogatories that would have disclosed identity of party members), *vacated sub nom. Moore v. Black Panther Party* and *Smith v. Black Panther Party*, 458 U.S. 1118 (1982) (stating that the issue was moot); *Grandbouche v. Clancy*, 825 F.2d 1463, 1467–68 (10th Cir. 1987) (vacating discovery order requiring plaintiff to disclose membership list of organization opposed to federal income tax system).

157. *See generally 2TheMart.com*, 140 F. Supp. 2d 1088 (refusing to order disclosure of non-party John Does' identities because defendant in shareholder derivative suit did not need identities to argue that corporation's stock price fell due to anonymous Internet postings rather than defendant's own misconduct). Many states have codified the reporter's privilege in statutes that contain detailed threshold and balancing tests similar to the amendment which this article proposes. *See e.g.* Colo. Rev. Stat. Ann. § 13-90-119 (2001) (subpoenaing party must show that information is "directly related to a substantial issue" and "cannot be obtained by any other reasonable means" and that "a strong interest of the" subpoenaing party outweighs the news person's First Amendment interest in nondisclosure); Del. Code Ann. tit. 10, § 4323 (2001) (allowing judge to order disclosure of content of information reporter obtained from confidential source if "judge determines that the public interest in having the reporter's testimony outweighs the public interest in keeping the

B. Actual Malice

A second approach to balancing First Amendment rights and accountability is the familiar actual malice test established in *New York Times v. Sullivan*.[158] The rule, as further elaborated in *Gertz v. Welch*, adds a constitutional element to defamation cases by requiring public officials and public figures to prove by clear and convincing evidence that the defendant acted with actual malice, i.e., with knowledge of or reckless disregard for the falsity of the statement.[159]

At first glance, the actual malice rule might seem to have little relevance to judicial review of a John Doe subpoena. After all, the actual malice rule deals with liability, not standards for unmasking anonymous speakers. But the conflicting interests underlying the actual malice rule are quite similar to the interests in anonymity and accountability underlying cyberSLAPP suits. The Supreme Court justified the actual malice rule as a way to balance "the need for a vigorous and uninhibited press and the legitimate interest in redressing wrongful injury."[160] In other words, the Court was balancing First Amendment interests against accountability interests.

Given this similarity, courts should take guidance from the manner in which the actual malice rule helps courts evaluate the state interest supporting defamation law. The mere fact that a plaintiff has *filed* a defamation claim does not establish a valid state interest in accountability. Instead, courts measure the weight of the state's interest in relation to the merits of the plaintiff's claim. Thus, if a public official or public figure can prove not just the common-law elements of defamation, but also that the defendant published the false statement with actual malice, then the state's interest is sufficient to overcome the First Amendment interest in free speech.[161] Only after such a showing will a court find that the defendant's speech was defamatory and therefore not protected under the First Amendment.[162]

---

information confidential;" statute directs judge to consider importance of issue to which information is relevant, efforts to obtain information from alternative sources, evidence available from alternative sources, and likely effect of disclosure on future newsgathering); D.C. Code Ann. § 16-4703 (2001) (court may compel disclosure of information only if party seeking disclosure "establishes by clear and convincing evidence that" the information is relevant and unavailable by alternative means and there is an "overriding public interest in the disclosure"); Fla. Stat. § 90.5015(2) (2001) (party seeking disclosure must "make a clear and specific showing that" information is relevant and material and cannot be obtained from other sources and a "compelling interest exists for requiring disclosure of the information").

158. 376 U.S. 254 (1967).

159. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

160. *See id.* at 341–42.

161. *See id.* at 343.

162. *See id.*

The same principle should help courts evaluate a cyberSLAPP plaintiff's interest in obtaining John Doe's identity. Courts should not simply assume a valid state interest from the mere fact that a cyberSLAPP plaintiff has sued John Doe, even if the plaintiff pleaded a valid claim. Instead, they should examine the merits of the claim to determine that there is in fact a sufficiently weighty interest to justify depriving John Doe of the right to speak anonymously.

C. Proposed Standard for Reviewing John Doe Subpoenas: Prima Facie Evidence and Balancing of Interests

The courts and Congress should recognize the First Amendment right to speak anonymously and should balance that right against the interest in compensating legitimate victims of actionable anonymous speech. To achieve any meaningful balance, the approach must involve some examination of the substantive merits of the claim against John Doe. This article suggests that Congress, or alternatively the courts, adopt the balancing test recently set forth by the Appellate Division of the New Jersey Superior Court in *Dendrite International, Inc. v. Doe*.[163]

The *Dendrite* test has three parts. First, the cyberSLAPP plaintiff's complaint must be sufficient to survive a motion to dismiss for failure to state a claim.[164] Second, the plaintiff must make a threshold showing of evidence to support a prima facie case.[165] As with the reporter's privilege and actual malice standards discussed above, this substantial review of the merits ensures that the cyberSLAPP plaintiff has a valid interest in accountability. Finally, if the plaintiff meets the requirements mentioned above, the court must balance the weight of the prima facie case and the need for disclosure against John Doe's interest in anonymity.[166] This careful calibration allows courts to protect John Doe's right to anonymity in cases where the cyberSLAPP plaintiff has a valid claim, but John Doe's identity adds little or nothing to that claim, as, for example, where John Doe is not a party.[167]

Merely requiring the complaint to survive a motion to dismiss does

163. No. A-2774-00T3, 2001 WL 770406 (N.J. Super. Ct. App. Div. July 11, 2000).

164. *See id.* at *1.

165. *Id.*

166. *Id.* The requirement would not, however, apply to any element that could not reasonably be proven without John Doe's identity. *Id.* For example, the trial court in *Dendrite* did not require the plaintiff to produce evidence of actual malice to support its defamation claim, because of the near impossibility of proving John Doe's subjective state of mind without even knowing his identity, let alone being able to cross-examine him. *See Dendrite Intl., Inc. v. Does*, No. MRS C-129-00, slip op., 15 (N.J. Super. Ct. Nov. 15, 2000).

167. *See generally 2TheMart.com*, 140 F. Supp. 2d 1088 (applying stricter standard of review for subpoenas seeking identity of non-party John Does).

not sufficiently protect John Doe's anonymity.[168] As demonstrated by *Dendrite* itself, a claim may satisfy the permissive Rule 12(b)(6) standard but still be doomed to fail as a factual matter.[169] Had the *Dendrite* court not required evidence of actual harm, the court would have deprived John Doe needlessly of his First Amendment right to speak anonymously so that Dendrite could pursue a claim for which it could never recover.[170]

Moreover, as shown by another recent New Jersey case, *Dendrite's* threshold and balancing test does not preclude valid claims. On the same day it decided *Dendrite*, the Appellate Division of the New Jersey Superior Court decided *Immunomedics, Inc. v. Doe*.[171] A poster calling herself "moonshine_fr" had posted messages on a Yahoo! message board discussing Immunomedics.[172] Moonshine_fr identified herself as an Immunomedics employee and stated that Immunomedics was out of stock for diagnostic products in Europe and was about to fire its European manager.[173] Immunomedics filed suit for breach of contract, breach of duty of loyalty, and negligently revealing confidential and proprietary information.[174]

Immunomedics subpoenaed Yahoo! for moonshine_fr's identity, and moonshine_fr filed a motion to quash.[175] In addition to moonshine_fr's messages, the company submitted evidence that all employees had executed a confidentiality agreement and that moonshine_fr's messages violated the agreement.[176] The trial court denied the motion to quash, reasoning that the evidence clearly supported claims for breach of the confidentiality agreement and duty of loyalty.[177] Affirming the trial court's decision, the appellate division repeated the standards it announced in *Dendrite* and held that Immunomedics had produced sufficient evidence to establish a prima facie claim for breach of the confidentiality agreement.[178] The court also held that Immunomedics' strong prima facie evidence that moonshine_fr was an employee, signed a confidentiality agreement, and breached that agreement outweighed

168. *See Dendrite Intl.*, 2001 WL 770406, at *12. "[A]pplication of our motion-to-dismiss standard in isolation fails to provide a basis for an analysis and balancing of Dendrite's request for disclosure in light of John Doe No. 3's competing right of anonymity in the exercise of his right of free speech." *Id.*

169. *Id.* at **13–14.

170. *See id.*

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

moonshine_fr's interest in anonymity.[179] So even the protective *Dendrite* standard does not preclude recovery when the plaintiff can prove a valid claim.

VI. CONCLUSION

A CyberSLAPP subpoena threatens to deprive John Doe of his right to speak anonymously without notice, judicial review, or any credible evidence of the claims against him. This is particularly troublesome because many cyberSLAPP plaintiffs seek only to discover John Doe's identity, not to obtain a judgment against him. In such cases, without meaningful notice and substantive review of the plaintiff's claim, the game is over before John Doe even knows it has begun.

The notice and prima facie evidence standard established by the New Jersey court in *Dendrite International v. Doe* offers a persuasive model for other courts that will soon have to decide how to balance anonymity and accountability. Nevertheless, John Doe's right to anonymity will receive inconsistent protection in the various states. To safeguard the right to anonymous online speech, Congress should adopt the ECPA amendment proposed in the Appendix. The amendment would preserve John Doe's due process rights to notice and a hearing, prevent the unnecessary infringement upon John Doe's anonymity, and still preserve a remedy for plaintiffs with substantial claims.

Eventually, technological developments could moot the issue of John Doe subpoenas. The Internet architecture could evolve to prevent anonymity altogether. One might be able to learn any Internet user's identity with a single click, the way one can now read a Web page's HTML source code. Such a world of total identity would render John Doe subpoenas unnecessary.

Alternatively, and perhaps more plausibly, we could see the widespread use of "anonymizing" devices allowing users to shield their identities online. CyberSLAPP lawsuits may drive many Internet users to use such cloaking technologies. As Columbia Law School professor Eben Moglen observes, "anonymity is a valuable commodity in social terms, and it is hard to imagine that anonymity will not take vast steps forward in the years to come."[180] Widespread anonymity could skew the balance in favor of anonymity at the expense of accountability. Ironically, the abuse of cyberSLAPP claims today may leave future victims of online defamation without a remedy.

179. *Id.*

180. *See generally* Kaplan, *supra* n. 16.

APPENDIX: PROPOSED AMENDMENT TO 18 U.S.C. § 2703(C)

Title 18, section 2703(c)(1), is amended as follows:

Section 1: In 18 U.S.C. § 2703(c)(1)(A), by inserting after "Except as provided in subparagraph (B)" the words "and (D)".

Section 2: By inserting after 18 U.S.C. § 2703(c)(1)(C) the following new subsection:

2703(c)(1)(D)(i) A provider of electronic communication service or remote computing service shall not disclose personally identifiable information pertaining to a subscriber to or customer of such service, to a person seeking disclosure other than a governmental entity, unless ordered to do so by a court in a civil proceeding, provided that:

(a) a court may issue such an order only upon a judicial determination that (1) the person seeking disclosure has produced evidence to support a prima facie case on a claim or defense to which the personally identifiable information is directly relevant, and (2) the strength of the prima facie case and the need for disclosure outweigh the subscriber's or customer's interest in remaining anonymous;[181]

(b) the person seeking disclosure gives the subscriber or customer of such service at least thirty (30) days' advance notice of the court proceeding relevant to the issuance of the court order;[182] and

(c) the subscriber to or customer of such service is afforded the opportunity to appear and contest the claim of the person seeking disclosure.[183]

(ii) A court applying the standard described in subsection 2703(c)(1)(D)(i)(a)(1) shall not require a prima facie showing of elements that cannot reasonably be proven without the subscriber's or customer's identity.[184]

(iii) The person seeking disclosure shall be deemed to have given "reasonable notice" to a subscriber or customer if the person posts copies (or a hypertext link to copies) of all relevant pleadings and motions in a manner reasonably calculated to come to the subscriber's or customer's attention, and e-mails copies to all known e-mail addresses for the subscriber or customer. Any person who uses or attempts to use the means of providing reasonable notice under this subsection to discover a subscriber's or customer's identity shall be deemed to have violated this chapter, and therefore subject to the provisions of section 2707.[185]

---

181. See *supra* § V.C for a discussion of the proposed standard of review.

182. See *supra* § IV for a discussion of the proposed notice and hearing requirement.

183. *See id.*

184. *See supra* n. 24 and accompanying text.

185. *See supra* n. 120 and accompanying text.

(iv) For purposes of this subsection 2703(c)(1)(D), the term "personally identifying information" means information (including Internet Protocol address) which identifies a subscriber or customer as the author or originator of a particular electronic communication.