COMMENT

Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation

*Joshua R. Furman**

A recent advertising campaign by a national Internet Service Provider (ISP) depicts a happy home of consumers who never have to leave their house thanks to their super-fast connection and the wonders of limitless shopping on the web. Television spots show people in awe over the selection and convenience as they click away at laptops purchasing kitchen appliances, trading stocks, and occasionally greeting a courier with the latest treat materializing from their online adventures. In some ways these ads are a fanciful depiction of our current reality. While many of us have felt the excitement of a dot com shipment just a few clicks away, the seamless function of technology and infrastructure depicted is probably a bit more idealized than we would recall. However, as we move closer to a society in which online activities increasingly usurp real world activities, we must ask whether fundamental rights will follow.

Consider the problem of John Doe, a member of our utopian cyber-shopping household, who wants to comment on a web forum

* J.D. Candidate 2002, Seattle University School of Law. Innumerable thanks are due to the staff of *Seattle University Law Review* whose commitment to enriching the legal community through exceptional scholarship is unparalleled. Many individuals have been of indispensable assistance in transforming this article from scraps on my hard drive to a printed reality. I would particularly like to thank Deirdre Mulligan and Alan B. Davidson as well as the entire staff at the Center for Democracy and Technology for their inspiration and example and Megan E. Gray at Baker & Hostetler Los Angeles for her comments and generous assistance with materials. Any spark of genius that the reader may be able to sift out of this piece is undoubtedly due to their contributions, while the copious errors glaring from every line are entirely my doing. Finally, to my family and friends who have stood with me throughout these trying times—my love and gratitude.

about an issue of public interest. Whether it is the stock of a publicly-traded company, a public figure, or a government official like a judge, when John Doe sends a critical anonymous post to the forum, he has just opened himself up to having his identity revealed to the object of his criticism. The company or individual need only file a defamation suit (with merit or otherwise) and proceed with discovery. It becomes readily apparent that when a netizen like John Doe wants to participate in an anonymous online discussion about an issue of public interest, he does so without the benefit of certain fundamental rights: free speech, privacy, or due process. This chills online speech, thus undermining the democratizing nature of the Internet.

I. INTRODUCTION

"[The Internet is] the most participatory form of mass speech yet developed." [1] Unfortunately, attacks on individual privacy in the courts threaten to chill participation in online speech. While all major online service organizations assure their subscribers that personally identifiable information is kept in some degree of confidence, such assurances must fail in the face of a court-ordered subpoena. Additionally, many companies disclose subscriber information without a court order: a civil plaintiff attorney's subpoena or request will often suffice. Often, subpoenas are served pursuant to lawsuits filed for the primary purpose of uncovering an individual's identity.[2]

Threats to individual privacy and speech online have recently been stressed in so-called cybersmear lawsuits.[3] These are defamation suits brought by companies against individuals who make disparaging remarks about a company on Internet discussion fora.[4] The processes, results, and consequences of cybersmear litigation serve as a touchstone for the issues presented by abuse of civil discovery against online John Does.

---

1. Reno v. ACLU, 521 U.S. 844, 863 (1997) (citing the lower court decision) (internal quotation marks omitted).

2. David L. Sobel, *The Process That "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J. L. & TECH. 3, 2 (2000) ("[C]ivil litigants are increasingly using the discovery process to pierce the veil of online anonymity.").

3. *Id.*; Donna Demac, *Cybersmears and Consumer Revenge Dot Com: Corporate Threats to Online Free Speech* (Aug. 2000), *available at* http://www.ncac.org/issues/cybersmears.html. *See also* J. Doe's Mem. in Supp. of Mot. to Quash Subpoena Issued to Silicon Investor/InfoSpace, Inc., *In re* 2TheMart.com, Inc. Securities Litigation (C.D. Cal. 2001) (No. SACV-9901127), *available at* http://www.aclu-wa.org/ISSUES/privacy/BB.Securities.Litigation.2.26.01.html; Compl. at 7, John Doe v. Yahoo!, Inc., (C.D. Cal. filed May, 2000) (No. CV-00-04993-NM (CTx)).

4. Blake A. Bell, *Plaintiff Corporations Face Resprisals from Cybersmear Defendants*, 14 NO. 8 CORP. COUNS. 1 (2000).

Lawsuits commenced for the purpose of identifying and silencing a cybersmear detractor are reminiscent of Strategic Lawsuits Against Public Participation (SLAPP).[5] SLAPP suits have long been recognized as an abuse of the judicial system. Sixteen states have statutes or strong case law prohibiting SLAPPs,[6] and federal courts, while not directly appealing to SLAPP doctrine, have used a similar approach under similar circumstances.[7] However, most analyses of First Amendment issues in cybersmear litigation have concentrated on the Free Speech Clause and not the Petition Clause implicated by anti-SLAPP law.[8]

This Comment questions the intellectual move away from SLAPP analysis of cybersmear cases. Although the emphasis on free speech has yielded some recent courtroom successes for online John Does, the defendants in these cases have been able to appear in court and assert their defenses.[9] Where defendants cannot appear to chal-

---

5. GEORGE W. PRING & PENELOPE CANAN, SLAPP'S: GETTING SUED FOR SPEAKING OUT 8–10 (1996) (stating that SLAPPs are suits filed as retaliation or reaction to defendant action under the Petition Clause where the suit would most likely chill or stifle that protected action).

6. California Anti-SLAPP Project, Other States: Statutes and Cases, *available at* http://www.sirius.com/~casp/menstate.html (last visited Apr. 18, 2001) (anti-SLAPP laws pending in many other states).

7. New York Times Co. v. Sullivan, 376 U.S. 254 (1964) (holding that to avoid chilling speech with frivolous lawsuits, standards of proof are higher in a libel action brought by a public official than a regular citizen); Bill Johnson's Restaurants Inc. v. National Labor Relations Bd., 461 U.S. 731 (1983) (holding that a retaliatory lawsuit filed against an employee by an employer is actionable as an unfair labor practice).

8. Commentators have summarily rejected analyzing cybersmear suits as SLAPPs on three grounds: (1) because they "refer[] only to suits based on 'communications made to influence a governmental action,'" Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 DUKE L.J. 855, 860 n.11 (2000) (citing PRING & CANAN, *supra* note 5); (2) because "this characterization ignores the power that the Internet gives irresponsible speakers to damage the reputations of their targets," *id.* at 865; and (3) because it "underestimates the potential benefits that defamation law may bring to Internet discourse," *id.* It should also be noted, however that the California Anti-SLAPP statute, CAL. CIV. PROC. CODE § 425.16, which this Comment analyzes to some extent, explicitly implicates the Free Speech Clause of the Federal and California State Constitutions. CAL. CIV. PROC. CODE § 425.16 (a)–(b)(1).

Additionally, courts have recently ruled that § 425.16 may apply in some cybersmear contexts. Hollis-Eden v. Angelwatch, (No. GIC 759462) (San Diego County Ct. Mar. 20, 2001) (Ruling on Defendants gpalcus and dickie13_62301's Special Motion to Strike and Motion to Quash Subpoena) (holding that posting on a Yahoo! message board about a publicly traded company is speech concerning a matter of public interest for the purposes of § 425.16); Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261, 1266 (C.D. Cal. 2001) (holding that anti-SLAPP provisions apply to statements made on Raging Bull Message Boards (http://www.ragingbull.com/community/) and that defendants making such statements are exercising their free speech in connection with a public issue).

9. Jeffrey Benner, *Chat Room Rants Protected*, WIRED (Feb. 27, 2001), *available at* http://www.wired.com/news/politics/0,1283,42039,00.html; Jeffrey Terraciano, *Can John Doe Stay Anonymous?*, WIRED (Feb. 21, 2001), *available at* http://www.wired.com/news/privacy/0,1848,41714,00.html.

lenge the sufficiency of the complaint on free speech grounds, SLAPP analysis provides a procedural mechanism for stopping frivolous lawsuits before the defendant's identity may be sought regardless of whether the defendant can appear. While it is true that the original purposes of the anti-SLAPP movement were grounded in strict Petition Clause issues, where the initial communication was "made to influence governmental action or outcome,"[10] current law and thinking have broadened that criterion to include the greater scope of the Petition Clause as a protector of public speech.[11] Under a broader definition, a First Amendment analysis of cybersmear must include not only free speech but also SLAPP considerations.

Instead of proposing a courtroom strategy per se, this Comment suggests that the SLAPP theory can function as a bar to abusive civil discovery by increasing the plaintiff's burden before issuance of a subpoena against a Doe defendant. Given the importance of the role that the Internet plays in facilitating communication and community building as well as the value we place upon free and open discourse, some regime of protection of anonymity must be instituted. In privately-controlled cyberspace, devoid of many of the constitutional protections of real space, procedural or substantive changes must be made in the law to protect subscriber privacy and preserve the participatory, and ultimately democratic, nature of the Internet.

This Comment will first survey the law of cybersmear, illustrating the paradigmatic issues and legal theories employed. Then, it will discuss the free speech issues and theoretical bases argued in court and legal journals, paying special attention to the shortcomings in current protection of defendant anonymity. Next, it will examine the value of online anonymity and the protections that the SLAPP theory offers. Finally, given the breakdown in the public and private space dichotomy, this Comment will argue for a new understanding of the SLAPP constitutional protections in cyberspace. This understanding will recognize the powerful dynamics of online speech regulation, in contrast with those of its real-world counterpart, and ensure that the would-be private arbiters of the technology and, therefore, liberty in cyberspace do not stifle the free discourse enabled by Internet technology.

---

10. PRING & CANAN, *supra* note 5, at 8.

11. For example, the California anti-SLAPP law, CAL. CIV. PROC. CODE § 425.16, protects "any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest." 5 WITKIN, CAL. PROCEDURE (4th ed. 1997) *Plead*, § 962, at 422. In addition, Pring & Canan themselves indicate that their limitation of the definition of SLAPP was to "provide a neutral, manageable, easily applied definition whereby even opponents can agree on whether a case is a SLAPP or not," PRING & CANAN, *supra* note 5, at 9, as opposed to being entirely true to the Petition Clause.

II. CYBERSMEAR AND THE PIERCING OF ANONYMITY

A. The Cybersmear Phenomenon

In recent years, a vast industry of service and content providers has taken shape in order to meet the demands of Internet users who seek out, read, and post information for others to read on an infinite number of topics. Among the most popular topics are the achievements and shortfalls of publicly traded companies. Various web sites, Usenet newsgroups, and chatrooms are dedicated to the discussion of stocks. In most of these fora, visitors with a wide range of expertise post messages touting or criticizing the performance, management, or employees of a given company. These messages are usually brief and exaggerated, often consist entirely of hyperbole or sarcasm, and range in tone from insults and name-calling to sycophancy. They are usually posted pseudonymously by users whose pseudonyms bear no relation to their actual names. Most visitors to message boards know to take anything they read with a grain of salt, as there is typically no way to verify the identity of the poster nor the truth of the statement.

For example, Yahoo!, a web-based content provider, hosts typical message boards on their web site, http://messages.yahoo.com.[12] Posters sign up for pseudonyms that do not require them to divulge any personally identifiable information (although their Internet Protocol addresses (IP addresses)[13] are tracked), and they can post messages to any of Yahoo!'s message boards which include a topic on each publicly-traded company.[14] Posters on Yahoo! message boards often make outrageous claims about the information that they have or about their position within a particular company. Most visitors are completely aware of the unreliable nature of these posts, and Yahoo! itself has a

12. Yahoo!'s message board topics run the gamut from computers to politics to sex. Their stock message boards, however, listed by industry category and company stock symbol at http://messages.yahoo.com/yahoo/Business___Finance/Investments/Sectors/, are among the most contentious. Other popular stock message boards include Raging Bull (http://www.ragingbull.com), The Motley Fool (http://www.fool.com), and Silicon Investor (http://www.siliconinvestor.com).

13. An Internet Protocol address (IP address) is the number assigned to a computer on the Internet. The protocols running on Internet servers and routers use IP addresses to direct information between computers. *See* WEBOPEDIA, *IP address*, *at* http://www.webopedia.com/TERM/I/IP_address.html (last modified Dec. 22, 1997); Chuck Semeria, *Understanding IP Addressing: Everything You Ever Wanted To Know*, (Apr. 26, 1996) *at* http://www.3com.com/solutions/en_US/ncs/501302.html.

14. *Yahoo! Message Boards*, *available at* http://messages.yahoo.com/reminder.html (last visited Jul. 16, 2001).

disclaimer which warns visitors to assume that no one is who they say they are.[15]

Despite the growing understanding among the Internet community that message boards are, at best, of questionable factual value, companies that have been disparaged on Yahoo! message boards or other fora have filed numerous defamation suits against the unknown John Does who posted critical or insulting messages.[16] These cybersmear cases ostensibly seek to recover for reputational damage allegedly caused by a message board post.[17] The primary purpose of many of these suits is not to pursue a defamation cause of action, however, but to reveal the identity of the poster and quiet criticism.[18]

This practice is becoming increasingly popular among corporate plaintiffs, raising several troubling issues. The most significant issue is the lack of privacy afforded to subscriber information by the courts. Subscriber information that is knowingly revealed to an online service provider[19] is not protected under the Fourth Amendment because there is no expectation of privacy.[20] Additionally, subscriber information is typically not protected by civil procedure.[21] Finally, subscriber

---

15. *Id.*

16. One report says that over 70 cybersmear suits were filed in 1999-2000 alone, although the number is likely much higher. Carl S. Kaplan, *Judge Says Online Critic Has No Right to Hide* (June 9, 2000), *available at* http://www.nytimes.com/library/tech/00/06/cyber/cyberlaw/09law.html.

17. Jay Eisenhofer & Sidney S. Liebesman, *Caught by the Net: What to do if a message board messes with your client*, BUS. LAW TODAY, Sept.-Oct. 2000, at 42; Mark C. Pomeroy, *Cyberlibel and Cybersmears*, *available at* http://www.bricker.com/newsevents/articles/131.asp (Jan. 2000).

18. Howard Mintz, *'Cybersmear' Lawsuits Raise Privacy Concern* (Nov. 28, 1999), *available at* http://www.mercurycenter.com/svtech/news/indepth/docs/boards112999.htm; *see also*, Sobel, *supra* note 2.

19. This Comment uses the term "online service provider" broadly to refer to Internet service providers (ISPs), web message board hosts, and any other host or content provider who might maintain users' personally identifiable information.

20. United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that a defendant who enters into a subscription agreement with an ISP revealed all the information related to his IP address to a third party under the *Smith v. Maryland*, 442 U.S. 735 (1979), analysis; he therefore, "cannot now claim to have a Fourth Amendment privacy interest in his subscriber information."); United States v. Hambrick, 55 F. Supp. 2d 504, 507–09 (W.D. Va. 1999) ("Where . . . dissemination of information to nongovernment entities is not prohibited [by agreement], there can be no reasonable expectation of privacy in that information." *Id.* at 509).

21. The Federal Rules of Civil Procedure, for example, do not provide any guidance for dealing with John Doe defendants, but have been generally interpreted permissively in favor of plaintiffs. *See, e.g.*, FED. R. CIV. P. 4 (John Does not mentioned concerning instituting a suit), 45(b)(2)–(3) (again, not mentioned concerning subpoenas); Estate of Rosenberg v. Crandell, 56 F.3d 35 (8th Cir. 1995) (holding that suit permitted where reasonable discovery would likely reveal identity of unnamed party); Maclin v. Paulson, 627 F.2d 83 (7th Cir. 1980) (permitting fictitious names until identity could be learned through discovery); *but see* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578–89 (N.D. Cal. 1999) (holding that discovery cannot go forward against a Doe defendant without some degree of specificity in complaint).

information is not protected from civil discovery under the Electronic Communications Privacy Act (ECPA)[22] because the Act only protects against discovery by government agencies.[23]

As the courts have failed to protect user privacy, so have the policies of the corporations that control user information. Terms of Service and Privacy Policies that users must agree to are usually vague about the circumstances under which a company will disclose information.[24] While most online service providers try to assure users that their information will be used for very limited purposes, nearly all of them reserve the right to disclose personally identifiable information for "legal process." [25] This clause allows the online service provider to avoid liability for nearly any disclosure to an attorney. Therefore, in practice, privacy assurances by web content providers are illusory when it comes to civil discovery targeted at uncovering a user's identity.

B. Courtroom Strategies and Legislation that Protect Online Privacy from Civil Subpoenas

1. Groping for Online Privacy

Federal substantive law and the Federal Rules of Civil Procedure (FRCP), as well as the Constitution, provide privacy protections in both online and "real-world" contexts.[26] As is often the case, the sudden appearance over the past few years of parties trying to litigate these issues in the online context has clarified the protections provided

22. Pub. L. No. 99-508, 100 Stat. 1848 (1986), (codified as amended at 18 U.S.C. §§ 2510 *et seq.* (Supp. 1999)).

23. 18 U.S.C. § 2703 (c)(1)(C) (1994).

24. For example, Yahoo!'s privacy policy states that personally identifiable information may be released to a third party "under special circumstances, such as to comply with subpoenas or when your actions violate the Yahoo! Terms of Service." *Yahoo! Privacy*, http://privacy.yahoo.com/privacy/us/mb/details.html (last visited Jul. 16, 2001). Of course, one action that violates Yahoo!'s Terms of Service is posting defamatory material. *Yahoo! Terms of Service*, http://docs.yahoo.com/info/terms/ (last visited Jul. 16, 2001).

25. *Yahoo! Privacy Policy, available at* http://docs.yahoo.com/info/privacy/ (last visited Jul. 16, 2001); *see also, e.g., AT&T Privacy Policy, available at* http://www.att.com/privacy/ (last visited Jul. 16, 2001); *Privacy Policies, available at* http://www.earthlink.com/about/policies/privacy.html (revised Mar. 7, 2000); *The Motley Fool: Privacy Statement, available at* http://www.fool.com/community/register/privacystatement.htm (last visited Jul. 16, 2001); *Raging Bull, Inc has created this privacy statement in order to demonstrate our firm commitment to privacy, available at* http://www.ragingbull.com/privacy.html (last visited Jul. 16, 2001); *SI: Privacy Policy, available at* http://www.siliconinvestor.com/misc/privacy.gsp (last visited Jul. 16, 2001).

26. The Federal Trade Commission and the ECPA are among the forces at work here, as well as the notice requirements in federal procedure and the Fourth Amendment of the Constitution.

to consumers online; simply put, "a right to privacy is not generally recognized on the Internet."[27] This is so primarily because private corporations, which are not subject to the constitutional restraints imposed on government, control almost all the infrastructure and technology that make up the Internet.

As a bellwether of American cyber-citizenship, one of the first America Online (AOL) cases litigated under the ECPA, *McVeigh v. Cohen*,[28] illustrates the problem of corporate control of private information. In *McVeigh*, a Navy officer used his AOL account to communicate on a personal matter.[29] The recipient checked the officer's AOL profile, which included the officer's marital status as "gay,"and reported that information to naval authorities.[30] The Navy contacted AOL and, without telling AOL that it was a government agency or obtaining a court order, confirmed the officer's name and sexual orientation before discharging him for violating the "don't ask, don't tell" policy for gays in the military.[31]

While the *McVeigh* court found that the Navy had violated the ECPA, the plaintiff prevailed only because it was the government that sought to violate his privacy.[32] The Act explicitly excludes account information revealed to private companies from protection. Everyday, companies seek to invade consumers' privacy in much the same way as the government in *McVeigh*, but, by virtue of the simple fact that these companies are not government agencies, their attempts at discovery and requests for user information are not curtailed by any sort of accountability for consumers' privacy.

Besides the ECPA, other legal theories placing liability on companies that uncover private information rarely succeed. Central to many of the problems encountered by defendants is the fact that constitutional protections and the laws designed to enforce them only extend to government actions. As scholars are starting to argue, however, the government is no longer the arbiter of power in the online environment.[33] Private companies control so much of the information and means by which we live our online lives that government intrusions, with the exception of criminal investigations, are negligible concerns for the average user compared to the day-to-day intrusions by

27. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1614 n.22 (1999) (citing MICROSOFT PRESS COMPUTER DICTIONARY (3d ed. 1997)).

28. 983 F. Supp. 215 (D.D.C. 1998).

29. *Id.* at 217.

30. *Id.*

31. *Id.*

32. *Id.* at 220.

33. *See* Schwartz, *supra* note 27, at 1633–34.

private organizations.[34] Concerns over corporate intrusions are massive, however, and remain unaddressed. This section will examine the strategies of some of the recent and pending litigation in cybersmear cases and the intrusions into consumer privacy that accompany those cases. The primary areas of law are as follows: (1) Fourth Amendment protections against unreasonable search and seizure; (2) procedural concerns of notice and opportunity to quash subpoenas attempting to discover personally identifiable information; (3) the Electronic Communications Privacy Act; and (4) industry self-regulation through the use of terms of service contractual protections.

2. Fourth Amendment

The Fourth Amendment of the Constitution ensures "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[35] It also directs that warrants may only be issued with certain specificity.[36] Fourth Amendment protections apply to "criminal prosecutions and suits for penalties and forfeitures under the revenue laws."[37] In general application, the right to privacy is asserted under the Amendment when the information is held with a reasonable expectation of privacy, free from unreasonable government intrusion.[38]

There are two problems typically encountered by litigants attempting to apply a Fourth Amendment defense to discovery of personally identifiable information in a civil case. First, courts have given us pause to question whether information provided to online service providers is private information in the eyes of the law.[39] Second, the

---

34. A survey of the issues presented at the Center for Democracy and Technology's privacy page (http://www.cdt.org/privacy/) or the Electronic Privacy Information Center's Privacy.org (http://www.privacy.org) illustrates a concentration of privacy issues concerning the practices of private companies, not the government.

35. U.S. CONST. amend. IV.

36. The Fourth Amendment concludes, "Warrants shall issue, but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

37. Flint v. Stone Tracy Co., 220 U.S. 107, 174 (1911).

38. United States v. Dionisio, 410 U.S. 1, 8 (1973).

39. In earlier Fourth Amendment cases, the Supreme Court found that there was no privacy interest in data collected through day to day use of technology. *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 Nova L. Rev. 551, 557 n.12 (1999) (citing Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that individuals have no privacy interest in telephone numbers dialed from their homes); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that individuals have no reasonable expectation of privacy in financial records maintained by their banks)). Authors have been critical of the Supreme Court's interpretation of the Fourth Amendment with regard to privately held personally identifiable information:

Fourth Amendment is simply not applicable to civil suits because it proscribes actions of the government rather than those of private parties.

The Supreme Court provided the test for Fourth Amendment analysis in *Katz v. United States*.[40] In *Katz*, the Court held that Fourth Amendment protection could be sought only when "the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded space."[41] This rule was clarified in *California v. Greenwood*,[42] where the Court held that the individual seeking protection must manifest an objectively reasonable, subjective expectation of privacy.[43] The rule, as clarified, was applied in a criminal case to subscriber information held by an ISP in *United States v. Hambrick*.[44] The *Hambrick* court held that two conditions must be met before attempting to assert a reasonable expectation of privacy: "(1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure."[45] The court found that information collected by the ISP when a subscriber signs up for service is knowingly revealed to the ISP.[46] Information so revealed cannot be held with a reasonable expectation of privacy and, therefore, is not protectable as private information under the Fourth Amendment.[47]

Even if a civil defendant was able to demonstrate that the information was unknowingly revealed to the online service provider, an attempt to assert Fourth Amendment protections against search and seizure would still fail because the Amendment only protects citizens against invasions of privacy by the government.[48] Therefore, since

---

> The Court's application of this standard has proved particularly troublesome in the information privacy context. The Court has continually held that individuals have no privacy interest in information divulged to the private sector, even though modern society leaves citizens no option but to disclose to others, e.g., disclosure as a condition of participation in society and technology accumulating transactional data.

Berman & Mulligan, *supra*.

40. 389 U.S. 347 (1967).

41. *Id.* at 353.

42. 486 U.S. 35 (1988).

43. *Id.* at 39–43.

44. 55 F. Supp. 2d 504 (W.D. Va. 1999).

45. *Id.* at 507.

46. *Id.* at 508–09.

47. *Id.*

48. *See* Barnard v. Young, 720 F.2d 1188, 1189 (10th Cir. 1983) (holding that for a Fourth Amendment violation, the right of privacy must be breached by a state actor; a private attorney acting under color of a court-authorized subpoena is not a state actor). *Cf.* Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1091–92 (W.D. Wash. 2001) (holding that *a court ordered subpoena*, on the other hand, "even when issued at the request of a private party in a civil

constitutional privacy protections are not extended to Doe defendants in cybersmear cases, they have pursued other avenues.

3. Rules and Case Law of Civil Procedure

Plaintiffs in cybersmear cases must often bend the rules of civil procedure in order to proceed with discovery against a John Doe defendant. In the federal courts, Federal Rules of Civil Procedure 4 and 45 have notice requirements where notice must be given to the opposing party upon filing a lawsuit[49] or upon serving a court-ordered subpoena.[50] When the defendant is a John Doe, however, the plaintiff often cannot readily identify him or her, so the plaintiff and the court must skirt the notice requirements to proceed with the case.

Rule 4 requires that a civil plaintiff serve a defendant with a summons and a copy of the complaint within 120 days of filing lawsuit.[51] Federal courts have permitted a wide variety of service methods, including those of the local state, but service of process must always be reasonably calculated to effectuate actual service.[52] Courts have consistently dismissed cases where the plaintiff did not attempt to serve process in good faith, or failed to serve process without taking any and all reasonable steps to do so. However, where the identity of the defendant is unknown (as in cybersmear cases), courts often allow limited discovery to find out who it is.[53]

Although frowned upon in some circuits, and not provided for in the FRCP, courts generally allow suits filed under fictitious names ("John Doe") when it appears that reasonable pre-trial discovery will uncover the defendant's true identity.[54] The only limitations on this discovery device in federal court are the particular judge's disposition towards fictitiously-named parties and the concern that, when federal jurisdiction is based on diversity under 28 U.S.C. § 1332, the unnamed parties would destroy diversity.[55]

---

lawsuit, constitutes state action and as such is subject to constitutional limitations.") (citing New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964); Shelley v. Kraemer, 334 U.S. 1 (1948)).

49. FED. R. CIV. P. 4(c).

50. FED. R. CIV. P. 45(b).

51. FED. R. CIV. P. 4(c)(1)–(2), (m).

52. FED. R. CIV. P. 4(e)(1).

53. *See* David M. Epstein, Annotation, *Propriety of Use of Fictitious Name of Defendant in Federal District Court*, 139 A.L.R. FED. 553 (1999); John Schwartz, *Questions on Net Anonymity* (Oct. 17, 2000), *available at* http://www.nytimes.com/2000/10/17/technology/17ONLI.html.

54. The Ninth Circuit is especially unfond of fictitious names. *See, e.g.*, Molnar v. National Broad. Co., 231 F.2d 684, 687 (9th Cir. 1956) (holding that the practice of suing under fictitious names is not justified by the FRCP); Bryant v. Ford Motor Co., 844 F.2d 602, 615 (9th Cir. 1987) (Kozinski, J., dissenting) (citing *Molnar*).

55. *See generally*, Epstein, *supra* note 53.

The Supreme Court has long allowed fictitious names in complaints without changing the circumstances of the action. In *Pullman Co. v. Jenkins*,[56] the fact that not all defendants were specifically named in the action did not justify ignoring those defendants for diversity purposes. Not only did the Court allow the fictitiously-named defendant to remain a party, it denied the petitioner's attempt to remove the case on the basis of diversity without proving the unidentified defendant's diverse citizenship.[57]

This rule has been followed well beyond diversity issues. Discovery has also been permitted without previously finding the actual names of the parties in order to determine their identity. In *Estate of Rosenberg v. Crandell*,[58] the Eighth Circuit held that "an action may proceed against a party whose name is unknown if the complaint makes allegations specific enough to be ascertained after reasonable discovery."[59] Likewise, in *Maclin v. Paulson*,[60] the Seventh Circuit held that "the use of fictitious names for defendants has been routinely approved even without discussion . . . when, as here, a party is ignorant of defendants' true identity, it is unnecessary to name them until their identity can be learned through discovery or aid of the trial court."[61]

The plaintiffs in both *Rosenberg* and *Maclin* pled the facts sufficient to indicate that if the defendants were identified, the plaintiffs would have an actionable claim.[62] In *Maclin*, for instance, the plaintiff alleged that two unnamed police officers beat him, denied him the right to call an attorney, and unnecessarily delayed his trial.[63] The plaintiff provided the exact date of the alleged beating, indicated that the officers in question were the arresting officers, and gave the exact location of the alleged beating.[64]

State courts have been much more permissive in recent and pending cybersmear cases, allowing discovery with much less particularity in the complaint. In *Hvide v. Doe*,[65] the court allowed discovery even though the complaint did not identify all the screen names of the

56. 305 U.S. 534 (1939).
57. *Id.* at 540.
58. 56 F.3d 35 (8th Cir. 1995).
59. *Id.* at 37.
60. 627 F.2d 83 (7th Cir. 1980).
61. *Id.* at 87 n.4 (citing a wealth of case law to that effect).
62. *Rosenberg*, 56 F.3d at 36; *Maclin*, 627 F.2d at 86–87.
63. *Maclin*, 627 F.2d at 86–87.
64. *Id.* at 84.
65. No. 99-22831-CA01 (Fla. 11th Cir. Ct. amended complaint filed Feb. 17, 2000) (currently on appeal).

Does nor the allegedly defamatory postings.[66] Likewise, in *Xircom v. Doe*[67] and *Raytheon v. Doe*,[68] the trial courts permitted discovery to identify the people behind screen names who had posted allegedly defamatory messages.[69]

Implicit in the courts' ruling in favor of reasonable, limited discovery of the identity of a party is the notion that it is not necessary to give notice of commanded production to the unnamed parties.[70] Elsewhere in the online context, however, some courts have approached unopposed discovery with more caution. In the sua sponte decision of *Columbia Insurance Co. v. Seescandy.com*,[71] the court found that under the Ninth Circuit rule disfavoring unnamed parties, limiting the plaintiff's discovery against an unknown and unserved defendant is necessary in the interest of "foster[ing] open communication and robust debate. . . . People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity."[72] The court further held that in order to balance the need of injured parties to have their day in court against the "legitimate and valuable right to participate in online forums anonymously or pseudonymously,"[73] the plaintiff must (1) show that the defendant is an individual or entity that could be sued, (2) show all efforts they have made to serve process on defendant, and (3) satisfy the court that the complaint could withstand a

66. *Id.*; *see also* Brief of Amicus Curiae ACLU and ACLU of Florida at 4, 12 n.9, *Hvide v. Doe*; Kaplan, *Judge Says Online Critic Has No Right to Hide*, *supra* note 16.

67. No. Civ. 188724 (Calif. Super. Ct. Ventura County June 14, 1999).

68. No. 99-816 (Mass. Super. Ct. Middlesex County filed Feb. 1, 1999). *Xircom* was settled before an appeal of the subpoena was heard, *Raytheon* was withdrawn by the plaintiff after discovering the identities of the posting authors through subpoena.

69. Rebecca Fairely Raney, *Judge Rejects Online Critic's Efforts to Remain Anonymous* (June 15, 1999), *available at* http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html.

70. In addition to the initial notice and service requirements in the Federal Rules, notice to the opposing party is required when serving a court-mandated subpoena on a third party. The problem presented by plaintiffs' inability to serve process on Doe defendants is compounded by the intent of the compelled subpoena notice requirement. FRCP 45 states, "Prior notice of any commanded production of documents . . . before trial shall be served on each party." FED. R. CIV. P. 45(b)(1). The Advisory Committee Notes for this rule further provide that "[t]he purpose of such notice is to afford the other parties an opportunity to object to the production or inspection." FED. R. CIV. P. 45 advisory committee's note, 1991 Amendment, Subdivision (b). The notice requirement of Rule 45 cannot be fulfilled when the other parties are not known. The result is that Doe defendants are denied their opportunity to object to a court-ordered subpoena that seeks to discover their identity from an online service provider.

71. 185 F.R.D. 573 (N.D. Cal. 1999).

72. *Id.* at 578.

73. *Id.*

motion to dismiss.[74] Finally, after meeting these criteria, the plaintiff should file an appropriate request for discovery outlining its satisfaction of the three requirements and aimed at making actual service of process upon the defendant possible.[75] In *Seescandy.com*, a singular email address, a variety of aliases, and email correspondence were sufficient to show that the defendant was an individual who could be sued.[76] Also, a record of phone calls made to all available numbers, letters sent to all available addresses, and emails sent to all available email addresses were sufficient to satisfy the second element of showing all previous efforts.[77] Finally, the court stressed the importance of the requirement that the plaintiff make a showing that its claim could survive a motion to dismiss:

> A conclusory pleading will never be sufficient to satisfy this element. Pre-service discovery is akin to the process used in criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary here to prevent abuse of this extraordinary application of the discovery process. . . .[78]

Since the plaintiff in that case was suing for control of a domain name, its claims, including trademark dilution and false designation of origin, were well-supported by the allegations in the complaint, and the court ordered them to file discovery requests to determine the actual identity of the defendant.[79]

Seescandy.com brings two important concepts to the debate of pre-trial discovery against unnamed Doe defendants. First, the court justifies its four-part analysis by acknowledging that it must balance the needs of the allegedly injured party against the rights of the online anonymous speaker regardless of whether the latter has made an ap-

---

74. *Id.* at 578–80.

75. *Id.* at 580.

> Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible.

Id.

76. *Id.* at 579.

77. *Id.* (*Seescandy.com* is a domain name dispute, and the plaintiffs gleaned all of their contact information for the defendant from that provided in his domain registration with Network Solutions, Inc. (http://www.networksolutions.com)).

78. *Id.* at 579–80.

79. For the plaintiff's claims see *id.* at 575, the holding is at 580–81.

pearance.[80] Second, in applying the four-part analysis, the court limits the ability of the plaintiff to go on a fishing expedition by requiring a civil version of showing just cause before permitting discovery.[81] The recognition that the Internet, particularly in the context of discovery against Doe defendants, requires heightened procedural safeguards, is critical to just adjudication of online issues. The shift from physical to virtual reality has resulted in a shift in the power balance from government to private entities. The entity that controls the "space" makes the laws for the space, and cyberspace is almost entirely in the hands of the private industry.

In a flip-flop of the citizen/government power dynamic, the holding in *Seescandy.com* was followed by another district court in *Stewart v. F.B.I.*,[82] in which a citizen sued the federal law enforcement agency for violations of the Privacy Act[83] and under common law. In *Stewart*, the plaintiff named as defendants four John Does, who were allegedly informing the FBI of the plaintiff's activities. The court utilized the *Seescandy.com* test to determine if the case against the Does could proceed. The court found that the plaintiff failed to show (1) that the court would have jurisdiction over the Does, (2) that he had taken reasonable steps to ascertain identity, and (3) that he intended to discover the identity of actual individual.[84] Having failed the three "limiting principles" of the *Seesdcandy.com* criteria, the case against the Does was dismissed.[85]

At least one state court has adopted the *Seescandy.com* test for discovery against online John Does specifically in the context of cybersmear. In *Dendrite International, Inc. v. Doe*,[86] the first major cybersmear case on appeal, the appellate court analyzed the trial court's use of the *Seescandy.com* test and found that it was appropriate even though it resulted in more stringent requirements for plaintiff to prove a prima facie case than against a motion to dismiss.[87]

---

80. *Id.* at 578.

81. *Id.* at 579–80.

82. No. CV-97-1595-ST, 1999 U.S. Dist. LEXIS 18784 (D. Or. 1999), *order adopted at* 1999 U.S. Dist. LEXIS 18785 (D. Or. 1999).

83. 5 U.S.C. § 552(a) (1994).

84. *Stewart*, 1999 U.S. Dist. LEXIS 18784 at *6–12. The court made sure to note that the individual being subjected to discovery could not be an excluded party under the Federal Tort Claims Act. *Id.*

85. *Id.* at *6–7.

86. 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

87. *Id.* at 769–70.

In *Dendrite*, a poster with the screen name "xxplrr" posted three comments on Yahoo!'s Dendrite message board[88] theorizing that the company's president had altered its revenue recognition accounting procedures and deceptively structured contract income in order to please investors with escalating revenue.[89] A fourth message suggested that the president was unsuccessfully trying to sell the company.[90] On the basis of these messages, Dendrite sued xxplrr as John Doe No. 3 alleging defamation and misappropriation of trade secrets.[91]

Dendrite then sought discovery to ascertain John Doe No. 3's identity.[92] The trial court denied discovery against John Doe No. 3, stating:

> The Court has found that the principals [sic] outlined in the Seescandy.com case are applicable to the instant matter and provide the parameters to be used in this balancing of interests. Dendrite has not made a prima facie case of defamation against John Doe No. 3, as Dendrite has failed to demonstrate the falsity of each of the alleged defamatory statements and/or Dendrite has failed to demonstrate the that it was harmed by any of the posted messages.[93]

Though Dendrite pled the prima facie case sufficient to survive a motion to dismiss,[94] it did not plead facts sufficient to grant discovery when the defendant's anonymity is at stake.[95] Reviewing this seminal application of the *Seescandy.com* test to a cybersmear case, the appellate court stated, "application of our motion-to-dismiss standard in isolation fails to provide a basis for disclosure in light of [the defendant]'s competing right of anonymity in the exercise of his right of free speech."[96]

---

88. Yahoo! DRTE, *linked from* http://messages.yahoo.com/yahoo/Business_Finance/Investments/Sectors/Technology/Software_and_Programming/index1.html (last visited Sept. 15, 2001).

89. *Dendrite Int.*, 775 A.2d at 763.

90. *Id.*

91. *Id.* Dendrite sued a total of 14 John Does with allegations of breach of contract, defamation, and misappropriated trade secrets. *Id.* However, the appeal focused entirely on xxplrr, John Doe No. 3. *Id.* at 760.

92. *Id.* at 764.

93. Dendrite Int. v. John Does, No. MRS C-129-00, 22 (N.J. Super. Ct. Ch. Div. Nov. 23, 2000) (opinion on plaintiff's Order to Show Cause), *available at* http://www.citizen.org/litigation/briefs/dendrite.pdf.

94. Citing *Zoneraich v. Overlook Hospital*, 514 A.2d 53 (N.J. Super. Ct. App. Div. 1986), the court stated that a defamation complaint must include the alleged defamatory words (identified by Dendrite as xxplrr's specific postings), their utterer (xxplrr him- or herself), and the fact of their publication (they were on Yahoo!'s message board). *Dendrite Int.*, 775 A.2d at 770.

95. *Id.* at 769–70.

96. *Id.* at 770; *Dendrite Int.*, No. MRS C-129-00, at 22 (finding insufficient evidence "that would warrant this Court to revoke [defendant's] constitutional protections").

4. Electronic Communications Privacy Act

The ECPA recognizes the need for enhanced privacy protections in the online environment. In order for electronic communications or subscriber information to be disclosed to a government entity under the Act, the entity seeking disclosure must obtain a court order or similar warrant under the Federal Rules of Criminal Procedure.[97] That order will be issued only if "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought are relevant and material to an ongoing criminal investigation."[98] This requirement of some showing of fact is similar to the requirements articulated by the court in *Seescandy.com*. More similar is the operative result that abuse of the ability to obtain disclosure is cut short by not allowing it without some demonstrable relation to an actual, litigable or prosecutable issue.

While the ECPA does limit private parties' disclosure of electronic communications, such limitation does not extend to restrict disclosure of subscriber information to private parties: "a provider of electronic communications service or remote computing service may *disclose* a record or other information pertaining to a subscriber or to a customer of such a service . . . to any person other than a government entity."[99] In *Jessup-Morgan v. America Online, Inc.*,[100] the plaintiff's attempt to show that AOL was liable under the civil penalty provision of the ECPA[101] failed because the party to which AOL had disclosed the plaintiff's subscriber information was not a government entity.[102]

Although *Jessup-Morgan* is not an example of abusive discovery, it demonstrates that the absence of any additional protections under the ECPA leaves open the possibility of abuse and does not provide for notice when subscriber information is requested. In *AnswerThink Consulting Group, Inc. v. Doe*,[103] the plaintiff filed a cybersmear defamation complaint against twelve unnamed Yahoo! message board posters. The plaintiff served subpoenas on Yahoo! and was given per-

97. 18 U.S.C. § 2703 (b) (1994).

98. 18 U.S.C. § 2703 (d) (1994).

99. 18 U.S.C. § 2703 (c)(1)(A) (1994).

100. 20 F. Supp. 2d 1105 (E.D. Mich. 1998).

101. 18 U.S.C. § 2707 (1994).

102. *Jessup-Morgan*, 20 F. Supp. 2d at 1108 ("AOL made the disclosure, not to the public, but to a private individual, [an] attorney, pursuant to a properly executed subpoena."). The record does not indicate that the attorney served a court-ordered subpoena; rather, this subpoena was most likely served by the attorney as an officer of the court pursuant to FRCP 45(a)(3). *Id.*

103. No. CV 00-03407-NM (CTx) (S.D. Fla. filed Feb. 23, 2000).

sonally identifiable information for the screen name Aquacool_2000.[104] It then filed a second suit to include Aquacool_2000's alleged actual name.[105] In the first lawsuit of its kind, Aquacool_2000 filed suit against Yahoo! for disclosing his subscriber information under circumstances that were inappropriate, despite being permissible under the ECPA.[106] In his complaint, Aquacool_2000 alleged, among other things, that Yahoo! acted improperly in (1) failing to make any efforts to give him notice of the disclosure of his personal information,[107] (2) accepting sub-standard service of subpoenas (by fax), and in (3) failing to make any efforts to confirm that the subpoenas were filed as part of a valid lawsuit when Yahoo! knew or should have known that many of the subpoenas it receives are issued under false pretenses or in contravention of state or federal law.[108] Ultimately, Aquacool_2000 argued that Yahoo! infringed on his free speech rights:

> Members who are the subject of frivolous defamation lawsuits and who later learn that Yahoo! has disclosed their information to third parties in response to subpoenas have their free-speech rights and rights anonymous speech unjustifiably chilled, to the detriment of the public at large by the dampening of the public debate caused thereby.[109]

To the extent that the ECPA does not prohibit the disclosure of subscriber information to a civil plaintiff, the adverse effect on speech that the Act was designed to protect remains.[110] If the privacy invasions that chill open expression on the Internet are to be avoided, additional rules must be put in place to prevent abuses not only by the government, but by private industry as well.

5. Contract—Terms of Service and Privacy Policies

All major online service providers have contractual terms that the user must agree to before using the service. Usually consisting of a Terms of Service (TOS) and a Privacy Policy, these contracts afford

---

104. Compl. at 8, John Doe v. Yahoo!, No. CV-00-04993-NM (CTx) (C.D. Cal. filed May, 2000).

105. Carl S. Kaplan, *In Fight Over Anonymity, John Doe Starts Slugging* (June 2, 2000), *available at* http://www.nytimes.com/library/tech/00/06/cyber/cyberlaw/02law.html.

106. John Doe v. Yahoo! Inc., No. CV-00-04993-NM (CTx) (C.D. Cal. filed May, 2000).

107. Yahoo!, as of May 26, 2000, claims to provide prior notice of disclosure. *See* Brian Livingston, *Policy change at Yahoo causes "identity crisis"* (May 26, 2000), *available at* http://news.cnet.com/news/0-1278-210-3287287-1.html.

108. Compl. at 6, *Doe v. Yahoo!*, No. CV-00-04993-NM (CTx) (including the allegations of (1) Invasion of Privacy, (2) Breach of Contract, (3) Negligent Misrepresentation, and (4) Unfair Competition and False Advertising).

109. *Id.* at 7.

110. *See* 132 CONG. REC. 14,441 (1986).

little protection to users when a third party subpoenas subscriber information.[111] A brief survey of TOS and Privacy Policies of industry leading online service providers reveals that all provide exceptions to privacy protection for "legal process" or other circumstances with varying degrees of vagueness.[112] The following excerpt from Yahoo!'s Privacy Policy is typical:

> Yahoo! may also disclose account information in special cases when 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 or interference with (either intentionally or unintentionally) Yahoo!'s rights or property, other Yahoo! users, or anyone else that could be harmed by such activities. Yahoo! may disclose or access account information when we believe in good faith that the law requires it . . . .[113]

Policies such as Yahoo!'s provide no privacy protection whatsoever to users whose identities are sought in connection with a civil lawsuit. In addition, a brief examination of major financial message board hosts shows that only one online service provider's privacy policy surveyed included any provision for notice to be sent to a user before his or her personally identifiable information is disclosed.[114] Prior notice gives John Doe defendants an opportunity to challenge the subpoena of their personal information.

While online service providers might, in practice, provide more privacy protection than indicated in their privacy policies, the actual protection afforded to all users is minimal because there is typically no contract provision allocating further liability for privacy to the online service provider.[115] Yahoo!, for example, does not necessarily hold itself out as providing notice when subscriber records are requested, though they have publicized that their usual practice (now) is to do so.[116] Without an explicit notice provision, however, the user has no recourse against Yahoo! if the latter discloses subscriber information

---

111. *Supra* notes 23–24 and accompanying text.

112. *See supra* note 24 and accompanying text.

113. *Yahoo! Privacy Policy, available at* http://docs.yahoo.com/info/privacy/ (last visited Jul. 16, 2001).

114. That one host was stock message board site for Go2Net (now InfoSpace, Inc.), Silicon Investor, *[Go2Net®], available at* http://www.go2net.com/corporate/legal/ (last visited Jul. 16, 2001). The current disclosure section of the Silicon Investor privacy policy mirrors the text of the Go2Net policy, *SI: Privacy Policy, available at* http://www.siliconinvestor.com/misc/privacy.gsp (last visited Jul. 16, 2001).

115. *See* Livingston, *supra* note 107; Kaplan, *Judge Says Online Critic Has No Right to Hide, supra* note 16 (indicating that Yahoo!, AOL, and MSN provide notice).

116. *See* Livingston, *supra* note 107.

without notice. Further, the company has little legal incentive to be vigilant about its disclosures.

In *Doe v. Yahoo!*, the plaintiff sued Yahoo! for, inter alia, breach of contract, alleging that the company improperly disclosed the plaintiff's subscriber information in violation of its own privacy policy, as quoted above.[117] The plaintiff argued (1) that Yahoo!'s disclosure was not required by law, so Yahoo! was not acting in good faith when it gave disclosure; (2) that, even if Yahoo! was acting in good faith, the resulting deprivation of privacy rights and due process opportunity was in contravention of public policy; (3) that Yahoo! violated the covenant of good faith and fair dealing implicit in contract by disclosing personal information to a hostile party; and (4) that the TOS and Privacy Policies were contracts of adhesion and unenforceable as waivers of plaintiff's remedies.[118] In addition, the plaintiff alleged negligent misrepresentation, claiming that Yahoo! lulls its members into a false sense of security that their information is protected while routinely disclosing subscriber information.[119]

Although no ruling was issued on these allegations, commentators have agreed that subscribers who agree to TOS and Privacy Policies like Yahoo!'s do not have the privacy protections that they believe to enjoy. Part of the problem is the alien online landscape—individuals hold "privacy expectations" about the vulnerability of their conduct which are native to real space yet inapplicable to cyberspace.[120] Most people do not realize that privacy intrusions that would be unthinkable in the home are easily accomplished by many entities online. Another part of the problem is that users are desensitized to the loss of their privacy rights through consent in facing a constant stream of disclaimers and consent checkboxes that they must agree to in order to carry on life online.[121]

While online service providers might defeat the protections represented in their own Privacy Policies, they also fail to disclose their actual practices. Many providers apparently do make an effort to give advance notice to subscribers before disclosing the latter's informa-

---

117. *See also Yahoo! Terms of Service* ¶ 6.a., *available at* http://docs.yahoo.com/info/terms/ (last visited Jul. 16, 2001) (propagating defamatory content is prohibited by Terms of Service).

118. Compl. at 11, John Doe v. Yahoo!, No. CV-00-04993-NM (CTx) (C.D. Cal. 2000).

119. *Id.* at 12.

120. *See* Berman & Mulligan, *supra* note 39, at 556–68. The authors note that "storing . . . personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed. . . ." *Id.* at 567.

121. *See, e.g.*, Schwartz, *supra* note 27, at 1675–76 (arguing that one of the benefits of adopting default privacy rules and only seeking consent when a data-collector tries to go beyond those rules is that users would lend the consent more scrutiny).

tion, but almost all of the providers fail to give *assurances* of notice in their TOS and Privacy Policy.[122] This absence leaves subscribers with no enforceable right to notice, and service providers with free reign to forgo notice when convenient.

III. FIRST AMENDMENT ANALYSES OF CYBERSMEAR

A. Freedom of Speech

Nearly all commentators on First Amendment issues in cybersmear have concentrated on the free speech implications of these unique libel cases.[123] Defamation defenses on free speech grounds generally follow two theories: the opinion privilege and the public figure doctrine.[124] While the public figure doctrine has been applied to cyber and real space speech alike since the seminal case of *New York Times Co. v. Sullivan*,[125] the use of the doctrine in cybersmear has been criticized as not responsive to the unique abilities of the defendants in these cases to be heard and their relative recklessness vis-à-vis other media.[126] The opinion privilege, on the other hand, has not been so criticized thus far, although it too fails to preserve anonymity of the defendant.[127]

1. Public Figure Doctrine

The public figure doctrine extends from the *New York Times* case and its progeny.[128] The central principle in the public figure doctrine is that, in the interest of robust debate, the standard of proof should be higher for a "public figure" defamation plaintiff, who has "project[ed] himself into the arena of public controversy and into the very 'vortex of the discussion of a question of pressing public concern.'"[129] Thus,

---

122. In April of 2000, Yahoo! adopted a policy of notifying users when it receives a subpoena about them. Kaplan, *John Doe Starts Slugging*, *supra* note 105. However, this policy change was never reflected in their published privacy policy at http://privacy.yahoo.com/privacy/us/.

123. *See, e.g.*, Jeremy Stone Weber, *Defining Cyberlibel: A First Amendment Limit for Libel Suits Against Individuals Arising from Computer Bulletin Board Speech*, 46 CASE W. RES. 235 (1995).

124. *See, e.g.*, Lidsky, *supra* note 8.

125. 376 U.S. 254 (1964).

126. *See* Lidsky, *supra* note 8, at 917–19.

127. Lidsky, *supra* note 8. Professor Lidsky's article is notable for its suggestion that the opinion privilege is sufficient to protect online anonymous speech as well as its rejection of SLAPP as a viable theory to defend John Does against cybersmear claims.

128. W. WAT HOPKINS, ACTUAL MALICE: TWENTY-FIVE YEARS AFTER TIMES V. SULLIVAN 1–8 (1989); LAURENCE H. ELDREDGE, THE LAW OF DEFAMATION § 52 (1978).

129. ELDREDGE, *supra* note 128, § 52, at 275 (citing *Pauling v. Globe-Democrat Publishing Co.*, 362 F.2d 188 (8th Cir. 1966)).

public figure defamation plaintiffs are required to show actual malice; they must show that the defendant either knew his statement was false or recklessly disregarded whether it was false or not at the time it was published. The extent of the rule today is a result of *Curtis Publishing Co. v. Butts*, in which the Court held that a public figure need not be a public official but must have sufficient public notoriety to launch a counterargument.[130] In that case, the Court stated that a plaintiff could be as minimally public as a college football coach to be held to the actual malice standard.[131]

The problems with the use of the public figure doctrine as a solution for cybersmear are twofold. First, and most significantly, if the doctrine can be applied as a defense to be asserted in court, it does nothing to protect the defendants' anonymity.[132] Since abusive cybersmear cases are withdrawn following discovery, the defendant never even appears in court.[133]

2. The Opinion Privilege Online: An Empty Ideal

The opinion privilege holds somewhat more promise as a free speech solution to abusive cybersmear; however, the general disarray

---

130. 388 U.S. 130, 154–55 (1967).

131. *Id.*

132. Defendants who do not receive notice of the suit filed against them are unlikely to appear in court in their own defense. As plaintiffs ostensibly try to comply with civil notice requirements, discovery may proceed against Does "for purposes of service of process" and defendants' anonymity is compromised.

133. *See, e.g.*, Terraciano, *supra* note 9.

In cyberspace, commentators have suggested that the public figure doctrine should apply to anyone who engages in online debate. Mike Godwin writes, "If online conferencing means anything, it means fostering of outspokenness—in effect, every opinionated individual has a microphone and an audience. . . . It's almost trivially easy to become a public figure on the Net." MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 82 (1998). Further, many have pointed out that the relative ease of rebutting potentially defamatory statements online gives all netizens the public access firepower of a public figure. *See, e.g.*, GODWIN, *supra*, at 82 ("If some bozo writes one hundred lines of false statement and innuendo about your sex life and personal habits, you can write five hundred lines of point-by-point refutation." Godwin writes that his views lead to the conclusion that there would be no libel suits online: people would just hit the reply button instead. *Id.* He contrasts this conclusion with the way libel law did develop on the Internet, much to the consternation of civil libertarians. *Id.*); *see also* Weber, *supra* note 123, at 261 ("A libel plaintiff who can post counterspeech on the bulletin board where the defamatory statement appeared is thereby analogous to a public official or figure. Thus the actual malice standard should be constitutionally required for that plaintiff to recover damages.") (citing EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 80 (1994)). However, as a legal theory in general, authors have questioned whether an assumed public figure status recognizes the reality of power inequities that permeate from the real world. While any defamation victim might be able to post a reply, the extent to which that reply is effective in rectifying the harm, if any, of the original statement still depends on the "ability and willingness" of others to concern themselves with the reply. Michael Hadley, *The Gertz Doctrine and Internet Defamation*, 84 VA. L. REV. 477, 492 (1998).

of the opinion privilege makes reliance tenuous. Prior to *Milkovich v. Lorain Journal Co.*,[134] courts had constructed a fact/opinion dichotomy in defamation law that considered the context of a statement before assigning liability.[135] This dichotomy was rooted in the Supreme Court's infamous dicta from *Gertz v. Robert Welch, Inc.* that "[u]nder the First Amendment there is no such thing as a false idea."[136] *Milkovich* virtually obliterated the application of this dicta in the courts.

While not completely destroying the fact/opinion dichotomy in defamation law, the Supreme Court in *Milkovich* narrowed the definition of 'opinion' to near absurdity.[137]

> [T]he court declared that the statement "In my opinion Jones is a liar" can be just as damaging to the reputation of Jones as the statement "Jones is a liar." The first statement may imply a false assertion of fact because it invites the audience to assume that unstated defamatory facts undergird the author's assertion.[138]

The analysis of liability therefore shifted from extrinsic factors that might show that a statement was intended as that of fact or opinion to a somewhat protectionist stance towards the plaintiff. Under the *Milkovich* rule, the possible perception of defamatory meaning by a third party, rather than the intent of the defendant, is the issue. As a

---

134. 497 U.S. 1 (1990).

135. *See, e.g.*, Lidsky, *supra* note 8, at 922 (describing the influential four-factor approach of then D.C. Circuit Judge Starr: "(1) 'the common usage or meaning of the specific language of the challenged statements itself'; (2) 'the statement's verifiability'; (3) the linguistic context of the statement; and (4) 'the broader social context or setting in which the statement appears.'") (citing *Ollman v. Evans*, 750 F.2d 970 (D.C. Cir. 1984) (en banc)) (footnotes omitted).

136. 418 U.S. 323, 339 (1974). The quote concludes, at 339–40: "However pernicious an opinion may seem, we depend for its correction not on the conscience of judges and juries but on the competition of other ideas. But there is no constitutional value in false statements of fact."

137. *See, e.g.*, MARK SABLEMAN, MORE SPEECH, NOT LESS: COMMUNICATIONS LAW IN THE INFORMATION AGE 83 (1997).

> When the *Milkovich* case reached the U.S. Supreme Court, that Court laid down a new federal constitutional rule concerning liability for opinions: The more outrageous your opinions, in style and content, the more likely they are to be protected. This is an oversimplification, but not by much. The Court's ruling in *Milkovich v. Lorain Journal Co.* divided up the universe of opinion, a field that had been afforded nearly complete protection from libel laws. Commentary that uses concrete words and facts and understated expression—the kind that really makes you think—after *Milkovich*, can, for the most part, subject the speaker to a full-fledged multimillion-dollar libel suit. But overstated and grossly exaggerated rhetoric—even when it uses highly charged words like 'blackmail,' 'treason,' and 'rape'—remains fully protected.

Id.

138. Lidsky, *supra* note 8, at 924 (footnotes omitted).

result, only those statements that "cannot be interpreted as stating actual facts" are protectable under the First Amendment.[139]

In the absence of any contextual analysis of cybersmear statements, anonymous online authors on message boards strewn with high-strung hyperbole rarely have a chance to succeed with an opinion defense.[140] Simply put, given the tone of these boards, nearly any expression could be found actionable. Additionally, like the problem with the public figure doctrine, the opinion privilege must be asserted by the defendant in court. This requires the identity of John Doe to be revealed for notice purposes, destroying anonymity and obviating the goal of not chilling speech.[141]

B. Theoretical Underpinnings Supporting a Free Speech Analysis and Justifying Limitations on Defamation Defenses

It is not enough to know that online John Does are not afforded protection as a matter of course. An exploration of *why* reveals that free speech theory, as applied to defamation on the Internet, fails to recognize the unique nature of the medium in eliciting and maintaining dialogue and community. This section will venture onto this uncertain ground and illustrate the social and policy issues concerning First Amendment protections in cybersmear cases. Initially looking at

---

139. *Id.* at 928. On 929, she continues: "The Court's failure to specify what role context plays in determining whether a statement implies an assertion of objective fact is a critical flaw in its analysis." Indeed, the Court does not specify the role of context because it has no place in their strict analysis of the text of the allegedly defamatory statement.

140. Nat Stern has argued that *Milkovich* did little but clarify the opinion privilege in defamation, leaving the fact/opinion doctrine substantially intact. But even under his analysis, context of the statement at question can be ignored: "Once meaning is established, the resolution of opinion-cum-nonverifiability virtually always becomes self evident." Nat Stern, *Defamation, Epistemology, and the Erosion (But Not Destruction) of the Opinion Privilege*, 57 TENN. L. REV. 595, 615 (1990). Thus, he says, "verifiability often becomes intertwined with linguistic analysis." *Id.* However, even he admits that the overly formalist tendencies of this approach have their draw-backs: "Unduly facile judicial reliance on verifiability may vitiate proper analysis; or ostensibly verifiable statement [sic] may be classified as factual when a more intricate inquiry into context would disclose a less literal content." Stern, *supra*, at 615 n.147. Stern would be hard-pressed to show a similar disposition in the *Malkovich* majority. In fact, Justice Brennan dissents from the majority on the very issue of looking at the context of allegedly defamatory statements: "I part company with the Court . . . because I find that *challenged* statements cannot reasonably be interpreted as either stating or implying defamatory facts about petitioner." *Malkovich*, 471 U.S. at 25 (Brennan, J. dissenting) (emphasis added).

141. However, the opinion privilege does have the virtue of being raiseable as early as a motion to dismiss. *See* Lidsky, *supra* note 8, at 921. *But see* Sobel, *supra* note 2, at 3 ("[A]nonymity also plays an important role in fostering free expression. The protections of anonymity thus takes on added significance on the Internet. . . ."); Lisa M. Nijm, *The Online Message Board Controversy: Physicians Hit with Claims of Libel and Insider Trading by Their Employers*, 21 J. LEGAL MED. 223, 238 (2000) ("If the current trend of 'John Doe' cases continues, then the result will be a chilling effect on anonymous speech on the Internet.").

the justifications for defamation law, then continuing to the qualified privileges and their application online, this section will show the inadequacies of relying on free speech defenses both theoretically and pragmatically. The ultimate consequence of these inadequacies is that the beneficial aspects of the Internet as an open forum are jeopardized because of the chilling effect on speech brought on by lesser protections created for the print and broadcast media.

As noted above, commentators have analyzed the First Amendment issues of cybersmear almost exclusively in terms of the Free Speech Clause. The first substantive works touted the historic preservation of free speech freedoms in civil defamation as a baseline for limiting the liability of cybersmear authors.[142] Since then, additional normative arguments have been offered in favor of the free speech defense to defamation and limitations on that defense in the interests of maintaining a higher level of discourse on the Internet.[143] The predominant argument can be found in Professor Lidsky's defense of Robert C. Post's notions of defamation law[144] making meaningful discourse possible.[145]

The normative argument justifying the limitations of free speech analysis approaches the problem of cybersmear with the baggage of predetermined normative values for defamation as protector of reputation. Drawing on Post's analysis of reputation as property, as honor, and as dignity, Lidsky proposes a First Amendment regime for cybersmear based entirely on the opinion privilege. While she does argue for expanded First Amendment protections for online John Does, her predeterminations about relative valuation of expression constrain her opinion privilege to little more than allowed by *Milkovich*.

Although case law is concerned with the harmed dignity of the individual, corporate plaintiffs are ostensibly only concerned with financial gain. While particular corporate officers may have their egos bruised online, a corporate plaintiff, as the ultimate economically rational actor, pursues litigation only as long as it is good for business. This means that while a corporation might not have a sense of dignity per se, it does place a financial value in maintaining its reputation in the eyes of the public, especially in the context of its stock price.

---

142. *See* Weber, *supra* note 123, at 237. ("[T]he Court's logic for requiring actual malice protection is, at times, analogous to situations in which libel plaintiffs have been defamed by bulletin board speech.").

143. Lidsky, *supra* note 8, at 884 ("If John Doe is unscrupulous or merely reckless, however, he . . . can pollute the information stream with defamatory falsehoods.").

144. Robert C. Post, *New Perspectives in the Law of Defamation: The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CALIF. L. REV. 691 (1986).

145. Lidsky, *supra* note 8, at 886.

From this perspective, the decision whether to file a cybersmear suit is entirely a cost-benefit analysis weighing the likely costs relative to the gains and assets of the corporation. Since the corporation has much greater financial resources, Lidsky says, "[i]t is tempting to portray the new Internet libel suits as David versus Goliath battles, pitting ordinary John Does against powerful corporate interests out to intimidate their critics into silence."[146] But she argues that this is an inaccurate portrayal because "[i]n the online world, every John Doe is potentially a publisher" who, despite having the power to be heard by millions, exercises a startling degree of recklessness in standards of information to publish.[147]

Turning to Post, Professor Lidsky says that the potential for damage caused by John Does warrants limiting their free speech privileges in defamation law because limitation "has the potential to curb the excesses of Internet discourse and to make Internet discourse not just more civil but more rational as well."[148] This shift occurs through the chilling effect that defamation suits and the threat of defamation suits have on speech. Here, Lidsky recognizes the danger that these suits "may chill more than defamatory falsehoods,"[149] but concludes that this danger must be balanced against the fact that "[the suits] make Internet users more temperate and more cautious about making unsupported factual assertions"[150] and the ultimate worth of speech by John Does in cybersmear.[151]

In the determination of the value of cybersmear speech, the constraints imposed on online speech by reliance on the opinion privilege are most marked. By asserting that cybersmear speech has an inherent value that must be weighed (and implying that it would not be weighed heavily), Lidsky draws most heavily on Post's concept of defamation law protecting reputation as dignity. For Post, dignity is the opposite of individual autonomy because dignity is the result of understandings gained from social interactions while autonomy is the

146. *Id.* at 883.

147. *Id.* at 884.

148. *Id.* at 887.

149. *Id.* at 890. The sentence reads, "There is some danger, therefore, that the growing popularity of the new Internet libel suits may chill more defamatory falsehoods – it may also chill the use of the Internet as a medium for free-ranging debate and experimentation with unpopular or novel ideas." *Id.* (footnotes omitted).

150. *Id.* at 889.

151. *Id.* at 892 ("Thus, before lamenting the chill that defamation actions will have on the John Does who frequent financial message boards, it is worthwhile to explore whether their speech is *worthy* of First Amendment protection.") (emphasis added).

result of self-realized understandings.[152] Concepts of dignity are therefore inextricably linked to concepts of community.[153] Limitations imposed on speech in the name of dignity are then limitations in the name of preservation of community. The reasoning is that defamation law qua First Amendment behavior-norming boundaries also defines the boundaries of a society.[154] Exclusion of certain speech from First Amendment protection maintains the definition of the society from which that speech is excluded.[155] Ultimately:

> A community without boundaries is without shape or identity; if pursued with single-minded determination, tolerance is incompatible with the very possibility of a community. For this reason tolerance as an ideal is incomplete. If community life is to survive, on either the local or national level, tolerance must at some point or another come to an end. Exactly where that point is depends a great deal on the importance one attaches to the intensity of community life and to the exercise of freedom of expression as a reflection of individual autonomy.[156]

In the context of cybersmear, Professor Lidsky paints an equally bleak picture of the dangers of open boundaries of speech. Citing the King James Bible,[157] she elaborates:

---

152. This conception is to be contrasting with Justice Harlan's conception of dignity in *Cohen v. California*, 403 U.S. 15 (1971), where "[t]he constitutional 'premise of individual dignity'. . . is thus a form of individual 'autonomy.'" Post, *supra* note 144, at 734 (citing *Cohen*).

153. *See* Post, *supra* note 144, at 736. *But see Developments in the Law: The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1609 (1999) ("We have only begun to encounter the communities that cyberspace makes possible and to apply our legal principles and rules to the unique situations created by Internet-enabled interactions.") [hereinafter *Law of Cyberspace*].

154. *See* Post, *supra* note 144, at 736.

155. Says Post: "Only a thoroughly demoralized society can tolerate everything." *Id.* at 736.

156. *Id.* at 736–37.

157. I mention her source not only for a facetious illustration of the culturally dependant inspiration Lidsky draws from, but also out of genuine concern for the implications of this scholarship: her footnote presents a bona fide bible study. In the interest of fair play, I repeat her words:

> In the Tower of Babel account, the people of the earth began to build a tower "whose top may reach unto heaven." Genesis 11:4 (King James). When God saw the tower, he said:
>
> > Behold the people is one, and they have all one language; and this they begin to do: and now nothing will be restrained from them, which they have imagined to do. Go to, let us go down, and there confound their language, that they may not understand one another's speech
>
> Id. 11:6-7 (King James). The next verses reveal the aftermath:
>
> > The Lord scattered the people abroad from thence upon the face of all the earth: and they left off to build the city. Therefore is the name of it called Babel; because the Lord did there confound the language of all the earth: and from thence did the Lord scatter them abroad upon the face of the earth.
>
> Id. 11:8-9

> But fostering a more participatory public discourse may come at a high cost. Speech from a 'multitude of tongues' may lead to truth, but it may also lead to the Tower of Babel. And the level of discourse on the financial message boards also suggests that fostering unmediated participation may make public discourse not only less rational and less civil; it also runs the risk of making public discourse meaningless. A discourse that has no necessary anchor in truth has no value to anyone but the speaker, and the participatory nature of Internet discourse threatens to engulf its value as discourse.[158]

This justification of the limitation of free speech protection in defamation allows protection of cybersmear defendants to be narrowed to the weak opinion privilege. Although Lidsky advocates a return of context analysis for online message board users[159] and urges courts to "take an active role in dismissing cases at an early stage,"[160] the limitations of this approach are clear: she offers no protections for the anonymity of John Does. She admits this much, but discounts the chilling effect of loss of anonymity as opposed to the threat of actual litigation.[161]

IV. GETTING THE 'CYBER' INTO CYBER-SLAPP

A. Technology and the Adaptation of Socio-Cultural Norms in the Law

While proponents of the opinion privilege in cybersmear argue for "courts to extend to the new class of Internet libel defendants all of the *existing* protections the First Amendment has to offer,"[162] commentators have long stressed that the onset of new technology necessi-

---

Lidsky, *supra* note 8, at 903 n.250.

And, to be somewhat facetious, is Lidsky representing that the morality of defamation law dictates that cybersmear lawsuits exercise their God-like power by throwing us into cybernetic confusion? Certainly not, if for no other reason than web content provider AltaVista has already resolved the larger issues of this problem. *AltaVista Translations, available at* http://babelfish.altavista.com (last visited Jul. 16, 2001).

158. Lidsky, *supra* note 8, at 902–03 (footnotes omitted).

159. *See id.* at 938–39.

160. *Id.* at 944.

161. *Id.* at 890 n.179 ("The solution that I advocate in this Article does little to alleviate the chill that flows solely from having one's identity revealed."). Professor Lidsky contrasts this chill with "the far more serious chill that results from being forced to defend against a meritless action." *Id.* However, in an amicus brief for *Hvide v. Does 1 through 8*, No. 99-2831 CA01 (Fla. Cir. Ct. 1999), she helped the ACLU argue that anonymity in cybersmear was a constitutional right. Brief of Amicus Curie American Civil Liberties Union and American Civil Liberties Union of Florida, Hvide v. Does 1-8, No. 99-2831 CA01 (Fla. Cir. Ct. dated Feb. 18, 2000) *available at* http://www.aclufl.org/hvideamicus.html. *See* Lidsky, *supra* note 8.

162. Lidksy, *supra* note 8, at 944 (emphasis added).

tates new rules of constitutional protections for speech. History provides innumerable examples of social and legal changes occurring in response to technological development. Just a few of the technological advances that provoked such change include the printing press, the telegraph, the radio and television, and now the Internet. However, in the case of the Internet, the adaptations of regulatory protections may not be keeping up with the adaptations of socio-cultural values and structures.[163]

Since theoretical bases for limiting defamation defense are rooted in concepts of community, let us first look at the new kinds of communities found on the Internet. Mike Godwin has proposed the "meme of virtual communities"[164] based in large part on Howard Rheingold's idea of "groupmind"[165] and the social scientists Roxanne Hiltz and Murray Turoff's study of "computer-mediated communication."[166] The genesis of the virtual community is the idea that the design of a communications system bears upon the development of the community of system users. Drawing heavily from their experiences on the WELL[167] system, Godwin and Rheingold describe a new set of community dynamics which define values by different means, although the actual elements of virtual community are not wholly unlike elements of traditional community.

As a gathering place for conviviality,[168] the Internet provides a level playing field where users can make up for the social nexus lost

---

163. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 1 (1983)

> Civil liberty functions today in a changing technological context. For five hundred years a struggle was fought, and in a few countries one, for the right of people to speak and print freely, unlicensed, uncensored, and uncontrolled. But new technologies of electronic communication may now relegate old and freed media such as pamphlets, platforms, and periodicals to a corner of the public forum. . . . The new technologies have not inherited all the legal immunities that were won for the old. . . . And so, as speech increasingly flows over those electronic media, the five-century growth of an unabridged right of citizens to speak without controls may be endangered.

Id.

164. GODWIN, *supra* note 133, at 52. Originating from the work of humanist biologist Richard Dawkins, a "meme" is conceptualized as a unit of cultural evolution. The archetypal meme is a self-replicating idea that flows from person to person transmitting itself and the cultural information it carries along with it. Memes thereby change social structures and conditions and create new social institutions as individuals come in contact with them. *See* THE FREE ONLINE DICTIONARY OF COMPUTING (Denis Howe, ed. 1993) *available at* http://www.foldoc.org.

165. HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER 110 (1994).

166. GODWIN, *supra* note 133, at 32.

167. Whole Earth 'Lectronic Link. The WELL was one of the early public computer conversation systems that went beyond the local range of dial-in Bulletin Board Systems.

168. RHEINGOLD, *supra* note 165, at 25.

when "the malt shop became a mall."[169] The Net grew as individuals and groups of individuals connected to each other in a medium that was, at first, highly structured, but unregulated and conducive to the free flow of ideas. But a medium and a nexus are not necessarily all that makes a community. Rheingold proposes that the shift from real world community to online community is something akin to Emile Durkheim's shift from *gemeinschaft* (premodern community) to *gesellschaft* (society).[170] Closely tracking Godwin's meme of virtual communities, the Durkheim shift is not a *product* of technological and social change, but an *effect* of changes manifesting in a "mass-psychological transition" where individuals internalize the technological and social structures produced by change.[171] The measure of the community, therefore, is that individuals "report . . . that they experience the feeling of being part of a community, and thus we should judge their claims of community membership seriously."[172]

The Durkheim model implies that communities, real or virtual, while defined and ordered to some degree by rules, cannot be changed by exterior powers that are not accepted and internalized by individuals within the community.[173] This assertion seems to run contrary to the possibility that the normative claim of the civilizing "benefits" of defamation law could be accurate.[174] Although, arguably, individuals online do internalize the effects of a few cybersmear suits as deterrence, the fact that real world laws and lawsuits exist outside of the social structure of the online community at least mitigates if not eliminates that effect.

One of the most important traits of the communities that do exist online is the facile capability to keep personal information private.[175] Professor Schwartz has called information privacy the second issue to the access problem of the digital divide in terms of importance for deliberative democracy online.[176] In order for democracy to be carried

169. *Id.* at 26.

170. *Id.* at 64–65.

171. *See id.* at 64; *see also* Larry R. Ridener, *Dead Sociologists' Index: Emile Durkheim – The Work*, *available at* http://raven.jmu.edu/~ridenelr/DSS/INDEX.HTML#durkheim (last visited Jul. 16, 2001).

172. *Law of Cyberspace*, *supra* note 153, at 1590.

173. RHEINGOLD, *supra* note 165, at 64 ("A science of Net behavior is not going to reshape the way people behave online. . . .").

174. *See* Lidsky, *supra* note 8, at 885–88.

175. I call this a "facile capability" because, while individuals engaged in discourse may be immediately anonymous to each other, their true identities are determinable. The resulting "anonymous feel" and perception of anonymous discourse creates operative, though not actual, anonymity. Better said, anonymity or pseudonymity is "something much more *possible* in cyberspace than in real space." *Law of Cyberspace*, *supra* note 153, at 1607 (emphasis added).

176. Schwartz, *supra* note 27, at 1651.

out online, individuals must be willing to speak. But individuals are dissuaded from speaking when their words and activities are tracked with no way for them to gauge who the trackers are and what information they are gathering.[177] In this way, the Internet is often referred to as a Hyde Park in London or the modern town square, where a speaker on a soapbox can have his piece and participate in discourse.[178]

"Without information privacy, however, the implications of congregating in the town square are dramatically changed."[179] The Supreme Court recognized the importance of anonymity in free and unfettered speech in the real world with *McIntyre v. Ohio Elections Commission*,[180] and a federal district court recognized its importance for cyberspace in *ACLU of Georgia v. Miller*.[181] In *Miller*, the court found that anonymity should be protected on free speech grounds because identity is a component of speech.[182] In so ordering, however, the court noted their purpose was to make sure that expression was not chilled.[183]

Miller turns an intellectual corner, in some sense, by opening the door on the relative value of anonymity in cyberspace. Anonymity in terms of personal privacy in the print world is well established, but when applying real world doctrine to cyberspace, Professor Katsh indicates that since "[i]t is clear that 'our paradigm of information *has been* the book,'" then "experiences in cyberspace, and the expectations and values fostered by this new environment, should be examined along with judicial assessments of the relevance of past decisions and experiences."[184] The newly-encountered qualities of information include the fact that electronic information is not constrained to the mortal coil of print—print spatial and temporal conceptions of expression do not apply.[185] "Cyberspace liberates information that had been effectively hidden or inaccessible under print's regime and may em-

177. *Id.* The Supreme Court has recognized this much and pledged to protect the "'vast democratic fora' of the Internet." *Id.* (citing *ACLU v. Reno*, 521 U.S. 844, 863 (1997)).

178. Schwartz cites Benjamin Barber as saying "the public needs its town square." *Id.* (footnotes omitted). Further, "In Benjamin Barber's vision, civil society is the free space in which democratic attitudes are cultivated and conditioned." *Id.* (footnotes omitted). *But see* Lidsky, *supra* note 8, at 885 ("'[A] civilized society,' as David Anderson has written, 'cannot refuse to protect reputation.'") (footnotes omitted) (alteration in original).

179. Schwartz, *supra* note 27, at 1652.

180. 514 U.S. 334 (1995).

181. 997 F. Supp. 1228 (N.D. Ga. 1997).

182. *See id.* at 1232.

183. *Id.* at 1233.

184. M. Ethan Katsh, *Rights, Camera, Action: Cyberspatial Settings and the First Amendment*, 104 YALE L.J. 1681, 1692 (1995) (emphasis in original).

185. *Id.* at 1704.

power groups or individuals whose communicative capabilities were economically restricted in print culture."[186]

The implications for defamation law are manifest and they are many-fold. While "uncivilized" discourse threatens whenever historically mute groups or individuals shake the boat of public perception, the entrance of new classes of speakers, and entirely new classes of speech, onto the scene requires that rules previously applied exclusively to the old classes be thoroughly re-examined. Given the unique nature of the Internet for fostering open and honest debate, the value of hearing the new speakers far outweighs any damage, dignitary or otherwise, that simply letting them speak without fear could do.

As a New York judge, invoking Justice Holmes's dissent in *Abrams*,[187] wrote:

> Do not underestimate the common man. People are intelligent enough to evaluate the source of an anonymous writing. They can see it is anonymous. They know it is anonymous. They can evaluate its anonymity along with its message, as long as they are permitted, as they must be, to read that message. And then, once they have done so, it is for them to decide what is "responsible", what is valuable, and what is truth.[188]

Applying this ideal to the Internet, Professor Schwartz predicted:

> Cyberspace has the potential to emerge as an essential focal point for communal activities and political participation. This development would help counter several negative trends in the United States. Voter turnout is declining; membership in many kinds of traditional voluntary associations is sinking; and a sense of shared community is frayed. Information technology in general and the Internet in particular have the potential to reverse these trends by forming new links between people and marshalling these connections to increase collaboration in democratic life.[189]

186. *Id.* at 1715.

187. Abrams v. United States, 250 U.S. 616 (1919).

188. State v. Duryea, 76 Misc.2d 948, 966 (N.Y. Supp. Ct. 1974). The Supreme Court also cites this perspicuous excerpt in *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 348 n.11 (1995).

189. Schwartz, *supra* note 27, at 1648 (footnotes omitted). One cannot help but note the record voter turnout in many areas for the 2000 presidential election and ask whether the proliferation of the Internet had any causal relationship.

B. Applying SLAPP to Cybersmear: The Last Vestige of Privacy

The change in the locus of social control, alluded to above, from the state to private service providers necessitates a change in our approach to privacy:

> From the earliest days of the Republic, American law viewed the government as the entity whose data use raises the greatest threat to individual liberty. . . . This approach means that treatment of personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before. These organizations' information processing contributes to their power over our lives. As the Internet becomes more central to life in the United States, the weaknesses and illogic of this existing legal model for information privacy are heightened.[190]

While cyberspace controls might exist almost completely within the grip of private ventures, the companies that earn their revenue from those ventures exist very much in the real world. In the real world, the state still has ultimate power. Though the state would most likely prefer to see online service providers police themselves, the state is ultimately responsible, by virtue of its power, for the conduct of these companies and the protection of each citizen's privacy.

To adequately protect online John Does from civil discovery proceedings, safeguards should be put in place to ensure that the values of anonymous speech are not compromised by frivolous, retaliatory litigants. Anti-SLAPP rules protect against just such lawsuits in the context of First Amendment petition rights.

Typically, SLAPP suits "are suits that chill, stifle and intimidate expressions by citizens attempting to participate in governmental activity and public policy."[191] Most anti-SLAPP laws prohibit suits that infringe upon a citizen's First Amendment right to petition the government for redress of grievances.[192] In California, home to one of the country's stronger anti-SLAPP laws, "[a] cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States or California Constitution in connection with a public issue shall be subject to a

190. *Id.* at 1633–34 (footnotes omitted).

191. California Anti-SLAPP Project, *Proposed Federal Anti-SLAPP Legislation* , *available at* http://www.sirius.com/~casp/halt.html (last visited Jul. 16, 2001).

192. The California Anti-SLAPP Project hosts a good deal of background information on the California law. *California Anti-SLAPP Project*, *available at* http://www.sirius.com/~casp/ (last visited Jul. 16, 2001).

special motion to strike."[193] This free speech language, also found in some other state statutes, broadens anti-SLAPP laws to cover plaintiff actions outside of a complaint, hearing or adjudicative process.[194] California case law, in combination with the above-quoted statute, § 425.16, indicates that protected speech includes all speech with any perceivable connection to a public, legal, or electoral process.[195] Additionally, there is "a well-established body of California case law which allows nonparties to civil litigation (such as a newspaper) to assert the constitutionally-protected rights of an author to remain unknown."[196] Presumably, this third party right would extend to online service providers as well as a newspaper.

In order for a plaintiff to survive a special motion to strike under § 425.16, the court must determine "that the plaintiff has established a probability that he or she will prevail on the claim," with the complaint and supplemental affidavits.[197] In *Wilcox v. Superior Court*,[198] the showing of "probability" of success was not satisfied by the cross-complainant despite the court's minimal requirements.[199] The court held that "reasonable probability of success means only that the plaintiff must demonstrate the complaint is legally sufficient and supported by a sufficient prima facie showing of facts to sustain a favorable judgment if the evidence submitted by the plaintiff is credited."[200] Although the cross-complainant argued that supporting facts need not be admissible evidence, the court stressed that the evidence must be submitted and therefore admissible or at least unopposed.[201] The cross-complaint was dismissed because it was wholly founded in hearsay.[202]

SLAPP suits are not only characterized by actions in relation to a pending authorized official matter. One characteristic that SLAPP plaintiffs share squarely with abusive cybersmear plaintiffs is that both easily hurdle the judicial barriers of failing to prevail on meritless suits because both have no intention of winning; rather, the costs of litiga-

193. CAL. CIV. PROC. CODE § 425.16(b)(1).

194. *See, e.g.*, DEL. CODE tit. 10 § 8136 (a)(3) (1994).

195. CAL. CIV. PROC. CODE § 425.16(a) ("this section shall be considered broadly"); CAL. CIV. PROC. CODE § 425.16(e)(3) ("any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest").

196. Rancho Publ'ns v. Superior Ct., 68 Cal. App. 4th 1538, 1541 (4th Dist. App. Ct. 1999).

197. CAL. CIV. PROC.CODE § 425.16 (b)(3).

198. 27 Cal. App. 4th 809 (1994).

199. *Id.* at 827–28.

200. *Id.* at 823.

201. *Id.* at 830.

202. *Id.*

tion are ordinary business costs in pursuit of business goals.[203] The subject matter of anti-SLAPP law being acts in furtherance of rights of petition or speech on a public issue is also similar to the defendant's speech in cybersmear.[204]

To the extent that there are subtle differences between the typical SLAPP action and its cybersmear counterpart, the normative values of taking full advantage of the democratizing nature of the Internet should be considered.[205] The benefits of online "John Doe-ism" must be balanced against the need of legitimate civil litigants to pursue action against their harmers. In the context of online anonymity, "it is clear that the balance should be weighed heavily toward the preservation of free and unfettered online expression."[206]

Anti-SLAPP laws as procedural rules are ideally suited to resolve issues of abuse cybersmear. If cybersmear plaintiffs have a burden to show that they have a probability of prevailing on the claim, frivolous suits will not be allowed to go forward. But that does not protect the defendant's privacy. SLAPP motions must still be brought by the defendant, necessitating his or her identification through plaintiff's attempts to comply with notice requirements, or at least ceding jurisdiction. Once again, a defendant who has not been notified of the proceeding cannot very well challenge a subpoena. If the defendant

---

203. Kathryn W. Tate, *California's Anti-SLAPP Legislation: A Summary of and Commentary on its Operation and Scope*, 33 LOY. L.A. L. REV. 801, 805 (2000) ("A SLAPP plaintiff. . . expects to lose and is willing to write off litigation expenses (and even attorney's fees where necessary) as the cost of doing business. Thus, the existing safeguards did not serve as a deterrent. . . .").

204. The allowable subject matter under the California statute has been a flashpoint of some debate. After initial litigation and amendments to the law, the defining ruling came from the California State Supreme Court in *Briggs v. Eden Council for Hope & Opportunity*, 19 Cal. 4th 1106 (1999), saying, in effect, that there must be an official proceeding involved on some level (The upshot of the decision, however, was that: "Under section 425.16, a defendant moving to strike a cause of action arising from a statement made before, or in connection with an issue under consideration by, a legally authorized official proceeding need not separately demonstrate that the statement concerned an issue of public significance." *Id.* at 1123). The court stressed that there was no bright-line rule for determining how, or if, a statement was related to a public issue, and a recent appellate ruling has held that as little as an issue's newsworthiness may determine if it is of public interest (*See* Marich v. QRZ Media, Inc., 73 Cal. App. 4th 299 (1999)). *See* Tate, *supra* note 203, at 825–28. The broadening of "public interest" in *Marich* is especially notable considering that the California State Supreme Court's ruling in Briggs narrowed the definition in spite of the legislative history of the unanimously approved 1997 amendment declaring: "the additional declaration of legislative intent would strengthen the statute against narrow readings of its protections. . . ." SENATE JUDICIARY COMM., SB 1296 BILL ANALYSIS (June 23, 1997) *available at* http://www.leginfo.ca.gov/pub/97-98/bill/sen/sb_1251-1300/sb_1296_cfa_19970516_131510_sen_floor.html.

205. In addition to simply balancing the relative values of speech and righting harms, it also bears noting that the democratizing mission of Internet regulation may bring some qualitative value on John Doe-ism to the equation.

206. Sobel, *supra* note 2, at 17.

cannot act on her own behalf (and we are assured that the plaintiff will not either), then the court must act to preserve the defendant's rights and prevent chilling of speech.

The model for such court activism can be found in *Seescandy.com* and *Dendrite*.[207] Anti-SLAPP statutes, *Seescandy.com*, and its progeny all allocate a substantially similar burden of proof to the entity seeking disclosure in the interest of protecting the rights of the entity about whom information is sought.[208] In *Seescandy.com*, the court required a minimal showing of facts to the end that the complaint under which the subpoena is sought is non-frivolous.[209] To overcome a motion to strike under an anti-SLAPP statute, the complainant must plead sufficient facts so that, if proven, the complaint would be sustained.[210] In each case, the essential burden is a prima facie showing that the disclosure is necessary for a valid reason. By these simple procedural mechanisms, courts have, to some degree, been able to weed out abuses of the power of the law to invade privacy.

The similar analysis engaged in by the courts in SLAPP and Doe defendant cases highlights the similarities in circumstances between the two situations. The antagonist in each situation is the entity or force that has the potential to upend the rights of an innocent party if abused. The courts, in both situations, have seen the potential for abuse and saw fit to mitigate that potential with additional limitations on the law or rule involved. While the necessity of limiting government action against the rights of citizens has long been a hallmark of American jurisprudence, the courts, in cases like *Seescandy.com* and *Dendrite*, have only recently recognized the equal or greater potential for abuse by private litigants and the need to curtail it.

---

207. In *Seescandy.com*, the court proceeded sua sponte, developing the four-part test for discovery against unknown defendants. *Supra* notes 73–77 and accompanying text. In *Dendrite*, the court applied the *Seescandy.com* test and declined to grant plaintiff's discovery request. *Supra* notes 82–92 and accompanying text.

208. James E. Grossberg & Dee Lord, *California's Anti-SLAPP Statute*, 13 COMM. LAW. 3, 5 ("The statute provides that the motion shall be granted unless a plaintiff 'establishes by pleading and affidavit a 'probability' of prevailing' on its claim.") (citations omitted); *Seescandy.com*, 185 F.R.D. at 579 ("plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss").

209. *Seescandy.com*, 185 F.R.D. at 578.

210. *See* Grossberg & Lord, *supra* note 208 at 5–6.

V. OTHER SOLUTIONS

A. Industry "Self-Regulation": Contract Solution

Since the relationship between consumer and corporation is primarily controlled by contract terms, reforms in privacy protection could start with self-regulatory moves to provide adequate contracts. Industry self-regulation has three benefits above government intervention: (1) the companies supplying the technology are in the best position to determine potential privacy threats and propose contractual solutions; (2) keeping in step with technological changes requires a speed of action that the corporate environment can maintain, but the government cannot; and (3) industry forces seek to avoid legislative action restricting their activities at all costs.[211]

In approaching the contract solution to privacy protection from civil subpoenas, two issues must be addressed. First, privacy policies must limit disclosure due to "legal process" to only court-ordered subpoenas. This requirement would help eliminate the practice of corporations filing frivolous suits aimed only at discovering the identity of online posters. Instead of plaintiff attorneys simply serving subpoenas as officers of the court, plaintiffs would be required to seek some degree of judicial approval to override privacy, which would screen out entirely frivolous cases. Second, privacy policies must allow for notice to subscribers prior to disclosure of their information. This would allow subscribers to challenge the disclosure and help to eliminate collusion between corporate plaintiffs and corporate online service providers.

B. Federal Mandate: Procedural and Substantive Law

While industry self-regulation may be the preferred method of approaching privacy issues, the shortcomings of contract reform on its own are fairly evident. First, even though requiring a court order to proceed with disclosure will add badly-needed judicial oversight to the subpoena process, the contract cannot determine the considerations that a court should undertake in granting that order. Second, it may be presumptuous to expect corporate interests to work together in good faith on behalf of the consumer. Regardless, it is obvious that whatever the contract between the online service providers and sub-

211. The public interest is not necessarily served by restrictions because restrictions can chill innovation and online freedom (as with encryption export restrictions), and the threat of legislative action can always be held over respective corporate "heads" to invoke action on their part, while legislative action, once taken, can typically be worked around.

scribers, it will have to work in concert with the courts to provide a comprehensive solution.

1. Changes to Federal Subpoena Rules[212]

Perhaps the most compelling solution is to change the rules of civil procedure to address the privacy requirements of the online environment. The judiciary has long grappled with the undefined gray area of Doe parties in federal court, and its responses have varied widely.[213] But there is a solid rule in case law for John Does online—*Seescandy.com* and the New Jersey appellate decision, *Dendrite*—as well as other federal cases like *2TheMart.com*. Changes to FRCP 45 that codify these holdings would most likely provide adequate privacy protections for online Does in federal court. As with the *Seescandy.com* sua sponte decision, the heightened criteria for discovery in online Doe cases places additional burden upon the court to identify the circumstances and apply the rule on its own volition. While this is somewhat unusual in our adversarial system, it is certainly not unheard of.[214] Courts have long provided special consideration and assistance for disadvantaged parties such as pro se litigants.[215] In keeping with that practice, changes in the Rules would give courts a more proactive role in discovery against Doe defendants.

First, Rule 45 should be amended to not allow blank subpoenas to attorneys where the defendant is unknown or known only by an online pseudonym. Second, the considerations for issuing a subpoena should be the four-part test for *Seescandy.com*,[216] similar to the ECPA restrictions on government-sought warrants, standards in SLAPP suits and constitutional protections. Third, should they become aware of the litigation through other means, Doe defendants must be permitted to make a special appearance to quash a subpoena that attempts to discovery their identity. Currently, an attempt to quash a subpoena cedes personal jurisdiction; however, defendants can make a special appearance to challenge personal jurisdiction. Still, discovery into the identity of a Doe is often necessary to show personal jurisdiction.

---

212. Although this section only addresses the federal rules, it does so with the consideration that most state court rules are analogous and that analogous changes in those rules would yield analogous benefits.

213. *See* Epstein, *supra* note 53.

214. Judicial oversight is extremely important in litigation against online John Does because of the great potential for abuse of the discovery process. *See* Sobel, *supra* note 2, at 21.

215. *See generally*, Julie M. Bradlow, *Procedural Due Process Rights of Pro Se Civil Litigants*, 55 U. CHI. L. REV. 659 (1988).

216. *See* Sobel *supra* note 2 at 22 n.35.

The need for a special appearance rule also shows the need for the fourth element—a notice requirement. Obviously, a defendant cannot appear to challenge a subpoena if she does not have notice that the suit has been filed or discovery commanded. While it would be unprecedented for the FRCP to require a third-party subpoena recipient to serve notice on a party to the suit, notice must be given by the online service provider to the Doe in order for the intent of Rule 45 to be fulfilled. The company being served is the only party that typically possesses the immediate means for contacting a defendant.[217] Under these circumstances, it would be much more helpful if the contract terms of the subscriber agreement provided for notice under these circumstances. While the court could order notice to be given by the online service provider, allocating the plaintiff's service of process burden to a third party is undesirable. Ideally, contract reform and procedure reform in this area would be symbiotic.

2. New Substantive Law

The fundamental problem with changing the FRCP as a comprehensive solution is that the Rules only apply in federal courts. There is no reason to think that cybersmear litigation is confined to the federal system; in fact, it may be more often litigated in the state courts.[218] Substantive federal law, however, could be applicable to all actions, federal and state. Substantive legislation aimed at protecting defendants like online John Does has already been enacted in the form of the ECPA. However, as stated above, these laws are only aimed at protecting against traditional Fourth Amendment violations. As such, they fall well short of protecting the privacy of civil defendants.

While the ECPA currently includes restrictions on civil discovery of electronic communications, subscriber information is explicitly not covered.[219] The call to expand the law's protections to limit civil discovery of subscriber information has already been sounded.[220] Previous suggestions include many of the solutions enumerated here, including requiring a court order for disclosure of personally identifiable information, requiring notice to the subscriber, and judicial over-

---

217. One court has pursued a different, novel solution to the notice problem; in *Dendrite Int.*, the trial court issued a sua sponte order for the plaintiff to post notice of the lawsuit on the message board where the offending comments were originally posted. *Dendrite Int.*, No. MRS C-129-00, at 8.

218. As noted above, cybersmear cases and their like usually have tort or breach of contract causes of action, usually only actionable in federal court with diversity jurisdiction.

219. 18 U.S.C. § 2703 (c)(1)(A) (1994).

220. Sobel, *supra* note 2, at 19.

sight.[221] But perhaps the most persuasive argument for substantive law protecting Does online is an already existing example—the protections granted personal data controlled by cable companies.[222]

The Cable Communications Policy Act of 1984 and the amending Cable Television Consumer Protection and Competition Act of 1992 included significant protections for subscriber information. In fact, the restrictions placed on law enforcement to get a warrant for personally identifiable information under the Cable Act are greater than those imposed by the ECPA. Under the Cable Act, a government entity can obtain a warrant if "(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim."[223] On the other hand, under the ECPA, a government entity must only present "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[224]

Further differentiated from the ECPA, the Cable Act places restrictions on civil discovery, authorizing disclosure "made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed."[225] The court order requirement and the notice requirement closely mirror desirable changes to the ECPA. In addition, case law interpreting the Cable Act has noted that Congress, in enacting the Act, was concerned with the privacy implications of "two-way" communications systems that can collect a great deal more information about subscribers.[226] Those types of legislative concerns lend themselves to online applications.

Litigation has found one chink in the armor that the Cable Act provides cable subscribers' privacy—lawsuits by cable companies against their own customers for pirating cable signals. In keeping with the legislative intent, courts have held that information collected by monitoring cable lines for the electromagnetic signatures of illegal de-

221. *Id.* at 19–21 (Sobel also calls for judicial discretion when the defendant has received notice but not made an appearance).

222. Schwartz, *supra* note 27, at 1675.

223. 47 U.S.C. § 551 (h) (note the notice requirement implicated by subsection (2)) (1994).

224. 18 U.S.C. § 2703 (d) (1994).

225. 47 U.S.C. § 551 (c)(2)(B) (1994).

226. Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874, 880 n.7 (10th Cir. 1992) ("[L]egislative history reveals that Congress was chiefly concerned with the privacy implications of two-way systems.").

scramblers (by means of a "Time Domain Reflectometer") is not necessarily personally identifiable information and can, at any rate, be disclosed in the prosecution of cable piracy without fear of liability.[227] This concern does not need to be dealt with here, however, as the technology that facilitates the Internet does not provide an analogous potential for piracy of Internet service or special devices to facilitate piracy.

A legislative solution of substantive law could clearly make way for the judicial oversight and notice required to protect John Doe privacy in civil discovery. However, as with each of the other solutions proposed, a substantive law solution has its weaknesses and is somewhat dependant on the other solutions. Undoubtedly, a parallel to the Cable Act for online service providers would be able to raise the bar on permissible subpoenas against a Doe defendant, but the notice element is still troubling. The Cable Act requires that the cable company give notice to the subscriber about the information it collects, but it does not prescribe a notice period for a challenge to the disclosure (although an "opportunity to contest" is called for when a government entity submits a subpoena, still a stronger rule than the ECPA).[228]

Also, there are significant differences between the Internet and cable television. First, cable companies tend to be the direct suppliers of cable content and services to the subscriber; as such, they have contact information such as an address and phone number that an online service provider might not have. Without that information, notice requirements are more difficult to comply with. For example, Yahoo! might only have an IP address as personally identifiable information. Second, even though cable systems may be seen as "two-way" systems, legislators may be less willing to apply strong protections to a media where the subscriber can conduct extensive activities and potentially harm others.

VI. CONCLUSION

Despite the wide variety of strategies that John Doe defendants and authors have put forward for protecting anonymous speech, courts do not consistently uphold users' privacy rights.[229] As a procedural

227. Metrovision of Livonia, Inc. v. Wood, 864 F. Supp 675, 681 (E.D. Mich. 1994).

228. 47 U.S.C. § 551 (a) (1994).

229. Recent court decisions are showing a certain propensity for protection of online speech and prohibiting cybersmear subpoenas by corporate plaintiffs on free speech grounds. *See* Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001)

> The Internet is a truly democratic forum for communication. It allows for the free exchange of ideas at an unprecedented speed and scale. For this reason, the constitu-

matter, anti-SLAPP doctrine employed by a pro-active bench provides a consistent basis for protecting not only a defendant's free speech rights, but his or her privacy rights. By preserving privacy, courts maintain the pseudo-anonymous environment that has allowed online speech to flourish. The social benefits of this speech are only beginning to be recognized, but the cost of limiting it is the chilling effect foreseen by many. Through understanding the nature of the Internet and the online community, social and legal regimes can develop and capitalize on anonymous speech, rather than perceive anonymous speech as a threat. As the possibilities for online commercial ventures seem to be crumbling, perhaps it behooves us to remember that when the Internet first became open to the public it was simply a forum for ideas, and users signed on to hear and be heard.

---

tional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded. Courts should impose a high threshold on subpoena requests that encroach on this right.

Id. at 1091 (with this justification, the court applied the *Seescandy.com* four-part test); Global Telemedia Int'l, Inc. v. Doe 1, 132 F. Supp. 2d 1261 (C.D. Cal. 2001).