

Corporate cybersmear: Employers file John Doe defamation lawsuits seeking the identity of anonymous employee internet posters

Authors: Margo E. K. Reder, Christine Neylon O'Brien

Persistent link: <http://hdl.handle.net/2345/1444>

This work is posted on [eScholarship@BC](#),
Boston College University Libraries.

Published in *Michigan Telecommunications and Technology Law Review*, vol. 8, pp. 195-217, 2002

Use of this resource is governed by the terms and conditions of the Creative Commons "Attribution-Noncommercial-No Derivative Works 3.0 United States" (<http://creativecommons.org/licenses/by-nc-nd/3.0/us/>)



**VOLUME 8
2001-2002**

MICHIGAN TELECOMMUNICATIONS AND TECHNOLOGY LAW REVIEW

**CORPORATE CYBERSMEAR: EMPLOYERS FILE
JOHN DOE DEFAMATION LAWSUITS SEEKING
THE IDENTITY OF ANONYMOUS EMPLOYEE
INTERNET POSTERS**

Margo E. K. Reder

Christine Neylon O'Brien

MTTLR

TM

COMMENT

CORPORATE CYBERSMEAR: EMPLOYERS FILE JOHN DOE DEFAMATION LAWSUITS SEEKING THE IDENTITY OF ANONYMOUS EMPLOYEE INTERNET POSTERS

*Margo E. K. Reder**
*Christine Neylon O'Brien***

Cite as: Margo E.K. Reder and Christine Neylon O'Brien, *Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking the Identity of Anonymous Employee Internet Posters*,
8 MICH. TELECOMM. TECH. L. REV. 195 (2002)
available at <http://www.mttl.org/voleigh/Reder.pdf>

INTRODUCTION	195
I. DENDRITE	198
II. DEFAMATION SUITS SEEKING TO UNMASK ANONYMOUS POSTERS	200
III. ANONYMOUS POSTERS PROTECTED BY ANTI-SLAPP LEGISLATION	202
IV. CONSTITUTIONAL PROTECTION OF ANONYMOUS SPEECH	204
V. PRIVATE SECTOR EMPLOYEE RIGHTS TO POST ANONYMOUSLY	206
VI. HOW THE INTERNET CHANGES THE RULES.....	209
A. <i>Freedom Fighters or Verbal Terrorists</i>	210
B. <i>Balancing the Equities: Employer Redress, Employee Speech and the Necessity of Disclosure—Developing a Standard</i>	211
CONCLUSION.....	217

INTRODUCTION

Consider the typical disgruntled employee's complaints: poor working conditions, bad management, long hours, low pay, limited opportunities for advancement, and so forth. Ten years ago, employee dissatisfaction was registered in limited ways—perhaps around the water

* Lecturer, Business Law, Wallace E. Carroll School of Management, Boston College.

** Professor, Business Law, Wallace E. Carroll School of Management, Boston College.
The authors wish to express their sincere appreciation to Dominic L. Blue and Louis S. Mercedes, both candidates in the J.D./M.B.A. program at Boston College, for all of their research and assistance on this project.

cooler, out in the parking lot, or during meals, conferences, etc. Such dissatisfaction usually occurred against the backdrop of downward trending economic conditions or significantly changing industry patterns. Very infrequently would this dissatisfaction register in publications such as company or industry newsletters, or in local or national news and magazine publications. Such complaints would, in this era, reach an audience limited both in scope and geography. In any event, the identity of the employee was known, or at least easily discoverable, so it was possible for the employer to serve process and file a complaint for any allegedly defamatory remarks.

This is a dramatic contrast to today's legal environment. Communications systems are now wide open and fully accessible, with no limits in range, scope or geography. Targeted audiences are accessible with pinpoint accuracy. Messages reach millions of readers with one click. There is a chat room for everyone.¹ Most importantly, there is no limit on content. Therefore, employees can register their dissatisfaction by posting a message in a chat room. Moreover, the identity of the posting employee is not easily discoverable due to anonymous and pseudonymous communications capabilities.² The nature of these online messages is qualitatively different from real-world communications. By way of example, newspapers have a responsibility regarding the veracity of the content that they print. Sponsors of online bulletin board services do not bear the same level of responsibility.³ In cyberspace chatrooms, everyone is a publisher; there are no editors. Online messages reflect this, too. The culture of online communications is vastly different from traditional discourse, in that the former tolerates and even encourages the use of hyperbole, crudeness, acronyms, misspellings, and misuse of language. It is a fast and loose atmosphere, emphasizing speed rather than accuracy.

This is the current environment in which anonymous employees post negative statements about their employers. The questions raised in this article relate to management's response, in the form of *John Doe* lawsuits, to this recent spate of negative Internet postings by employees.⁴

1. See <http://message.yahoo.com/?action=q&board=DRTE> (last visited Jan. 17, 2002) (posting for a message board for Dendrite International, Inc., discussed *infra* Part II).

2. E.g., <http://www.anonymizer.com/corporate/index.shtml> (last visited Jan. 18, 2002) (Anonymizer.com allows a person to navigate the Internet with privacy and anonymity).

3. Compare *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 339–348 (1974) (holding that newspaper publishers may be liable for defamation) with *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997) (holding that the Communications Decency Act of 1996 bars liability for computer service providers for statements made on its service by a third party).

4. See David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 Va. J.L. & Tech. 3 ¶¶ 10–17 (2000), at <http://www.vjolt.net/vol5/symp2000/v5ila3-Sobel.html> (last visited Sept. 2, 2001).

The emergence of the Internet as the medium of choice for such communications raises a myriad of questions that are new to courts. Questions arise regarding the extent to which employers may control the speech of current employees or former employees and, as a corollary to this, the extent to which such speech is protected, as well as whether this attempted speech control violates public policy. Such suits have just begun to reach the courts, and their resolution will form the contours of employee freedom of speech in the Internet age. *John Doe* suits implicate constitutional and common law issues ranging from the First Amendment to privacy, defamation, breach of employment agreement, and trade secret laws. Such suits involve statutes as well, including whistleblower protections and Strategic Litigation Against Public Participation ("SLAPP") laws.

Negative postings by employees also correlate to general economic conditions. During the current two year downturn in the financial markets, for example, there has been a tremendous increase in such postings. Employers have just begun to reply to these allegedly defamatory postings—in the form of *John Doe* lawsuits.⁵ Because it is difficult to discern who is speaking in cyberspace, plaintiffs often file a lawsuit listing "John Doe" as the defendant. Plaintiffs then invoke the power of a subpoena to compel the Internet Service Provider ("ISP") or Bulletin Board Service ("BBS") on which the posting was made to identify the poster, thereby unmasking these anonymous and pseudonymous individuals.⁶ It is worth noting that plaintiffs have an alternative course of action, in that they could investigate the postings and discover for themselves who is posting the messages. It is not clear whether any more effort or expense is involved in this strategy than immediately invoking the assistance—and the power—of the judicial system. But it is fair to say that involving the judicial system at this earliest stage is a coercive, and effective, strategy.

Armed with a subpoena—often issued even before a complaint has been filed—employers serve process on the posters' ISP/BBS directing them to divulge the identity of the poster. The vast majority of ISPs comply with such requests routinely and without challenge—and sometimes without the knowledge or consent of the posting subscriber.⁷ Courts are being asked whether they should authorize this expedited pre-service discovery to establish posters' identities sufficiently such that they may be served with process in accordance with the Federal Rules of Civil Procedure.

5. See Greg Saitz, *Walking a Fine Line on Cyber Rights: Dendrite Case at Core of Free Speech Battle*, STAR-LEDGER, Feb. 23, 2001, at 1.

6. See Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Disclosure in Cyberspace*, 49 DUKE L.J. 855, 880-83 (2000).

7. See Sobel, *supra* note 4, at ¶ 14.

I. DENDRITE

The fascinating aspect of pre-litigation subpoena cases is what happens next. Rather than continue with the lawsuit to test the merits of the contention that the postings were defamatory, a great number of companies that invoke the power of the judicial system to unmask the identities of the posters simply choose to fire the offending employee and drop the lawsuit. This naturally begs the question: what are the motives of the plaintiff companies—to be vindicated from the allegedly defamatory statements, or to silence their critics?⁸

The recent case of *Dendrite International, Inc. v. John Doe* highlights this phenomenon.⁹ The facts of *Dendrite* were typical of such cases. Defendants were four individuals who authored numerous messages posted under fictitious names on Internet message boards devoted to discussion of Dendrite International [hereinafter “Dendrite”]. The boards are maintained by Yahoo!, Inc., which refused to release the actual names of the alleged infringing users without a subpoena. The John Doe defendants were known only by their user names: John Doe No. 1 as “implementor _extraordinaire;” John Doe No. 2 as “ajcazz;” John Doe No. 3 as “xxplr;” and John Doe No. 4 as “gacbar.”¹⁰ John Does 1 and 2 stated in messages that they were current or former employees of Dendrite. As such, they were under contractual obligation not to disclose Dendrite’s proprietary or confidential information without permission for a period of two years from their departure, not to induce other employees to leave Dendrite, and not to engage in activities adverse to Dendrite’s interests.¹¹ John Does 3 and 4 denied ever working for Dendrite International.

The messages the four John Does posted discussed Dendrite in detail and the remarks were generally negative. John Doe 1 posted a number of messages. Dendrite claimed that in one he falsely accused the company of fraudulent business practices and alleged it had a policy of not paying bonuses. In another, Dendrite alleged that he claimed certain software products offered by Dendrite did not actually exist.¹² Dendrite claimed John Doe 2 posted a message which stated that “upper management has threatened to fire me and all of my co-workers at least once a week. We

8. See Sobel, *supra* note 4, at ¶¶ 15–17.

9. *Dendrite International, Inc. v. John Doe*, 775 A.2d 756 (N.J. Super. Ct. App. Div., 2001).

10. *Dendrite Int’l, Inc. v. John Does*, No. MRS C-129-00, at 1 (N.J. Super. Ct. Ch. Div., Nov. 23, 2000) [hereinafter “Dendrite I”] available at <http://www.citizen.org/documents/dendrite.pdf> (last visited Jan. 21, 2002), *aff’d*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

11. *Id.* at 2.

12. *Id.* at 2–3.

work this way daily.”¹³ John Doe 3 allegedly posted messages falsely stating that management was secretly and unsuccessfully “shopping” the company, and falsely stating that Dendrite had not been honest in its revenue recognition.¹⁴ Finally, Dendrite asserted that John Doe 4 “posted confidential information on certain accounts within hours of the company learning such information.”¹⁵

The relief Dendrite requested permitted a subpoena to be served on Yahoo!. Dendrite requested production of documents sufficient to identify the John Does. Yahoo! refused to release, absent a court order, the names of the defendants based on the company’s privacy policy. That policy states:

As a general rule, Yahoo! will not disclose any of your personally identifiable information except when we have your permission or under special circumstances, such as when we believed in good faith that the law requires it or under the circumstances described below. . . . 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 . . . anyone . . . that could be harmed by such activities.¹⁶

Dendrite asserted that individuals have no right to make defamatory statements, and that it had every right to protect its reputational interests. The John Does objected to Yahoo!’s release of such information, and urged that compelled identification interfered with their First Amendment right to anonymously express their opinions.¹⁷

Dendrite sought discovery from Yahoo! as part of an action for breach of contract (the employment agreements with John Does 1 and 2), breach of fiduciary duty, defamation, and misappropriation of trade secrets against the four defendants.¹⁸ It was alleged the defendants acted willfully and maliciously, and that their actions posed an immediate and continuing threat of harm to Dendrite International. The company also alleged that the postings contained per se defamatory statements, which falsely accused it and its management of fraudulent business practices.¹⁹

13. *Id.* at 3.

14. *Id.*

15. *Id.*

16. Dendrite Int’l, Inc. v. John Doe, 775 A.2d 756, 762 (N.J. Super. Ct. App. Div., 2001) [hereinafter “Dendrite II”].

17. See *Dendrite I*, *supra* note 10, at 18.

18. *Id.* at 1.

19. *Id.* at 1–2.

Dendrite further asserted that directly following these postings, there was a corresponding drop in the market price for shares of its stock.²⁰

Dendrite requested that the court enter an order granting it leave to conduct limited expedited discovery sufficient to identify the defendant John Does, so that it could serve them with the complaint and obtain an enforceable remedy.²¹ In order to identify the defendants, Dendrite needed to serve a subpoena on Yahoo! for the names, addresses, e-mail addresses and IP addresses of the defendants.

"As a general rule, discovery proceedings take place only after defendant has been served" with process.²² Courts have made limited exceptions to this rule, however, permitting pre-service discovery to learn the identifying facts necessary to permit service on anonymous defendants.²³ Recognizing the posters' legitimate rights of privacy and free speech, while understanding the rights of victims to receive redress through the judicial system, courts must carefully evaluate John Doe lawsuits in order to protect the interests of all parties.²⁴ The discussion at this point turns to further exploration of the parties, the causes of action, and defenses to them.

II. DEFAMATION SUITS SEEKING TO UNMASK ANONYMOUS POSTERS

Employer suits against employees who post messages anonymously are particularly worrisome because of the potential for extra-judicial action on the part of employers. The process is subject to abuse precisely because of the absence of an adversarial proceeding to determine whether plaintiffs are entitled to identifying information. In employer-employee cases, this situation is further exacerbated because of the parties' relationship. Defendants are not merely disgruntled shareholders or armchair critics; they earn their living in plaintiff's employ. Plaintiffs therefore wield enormous power over defendants beyond the judicial pre-service discovery proceeding. For example, plaintiffs in most cases have the unfettered ability to lower wages, worsen working conditions, or even fire defendants. Employers may have their reputations at stake, but corporate critics or whistleblowing employees have a great deal at

20. *Id.* at 4. Shares of Dendrite stock have traded in the range of 9 1/4–33 9/16 over a 52-week period, most recently closing at 13. *NASDAQ Composite Regular Trading*, WALL ST. J., Apr. 6, 2001, at C6. Dendrite recently authorized a share repurchase plan, perhaps in an effort to stabilize its share price. WALL ST. J., Feb. 1, 2001, available at 2001 WL-WSJ 2852846.

21. *Dendrite I*, *supra* note 10, at 5.

22. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 577 (N.D. Cal. 1999).

23. *Id.*

24. *See id.* at 578.

stake as well—they risk their livelihood even as they exercise their right of free speech. Unless the benefits of anonymous speech are somehow balanced against the potential for its abuse, such lawsuits will have a deleterious effect on constitutionally protected speech.

In order to silence their employee and investor critics, corporations have filed lawsuits under a variety of legal theories including defamation, trademark infringement, breach of confidentiality agreements and trade secrets, and tortious interference with contractual relations.²⁵ The theory most commonly used is defamation.

Generally, a cause of action for defamation in cyberspace consists of a published statement that libels the plaintiff and causes damage. The truth of the statement is an affirmative defense to a defamation action. Suits may also be defended based upon evidence that the published statements were merely hyperbole or opinion.²⁶ Differing standards based on the status of plaintiffs have developed to discern whether there is an actionable claim. For example, if the plaintiff is a private figure, he or she must prove only negligent publication of the false statement.²⁷ If the plaintiff in the defamation action is a public figure or public official, however, there is a requirement of actual malice in the publication of the statement. The current rule regarding defamation of public figures is based on the United States Supreme Court decision in *New York Times Co. v. Sullivan*.²⁸ There the Court held that a plaintiff who is a “public official” might succeed in a defamation action only if the plaintiff establishes that the defamatory statement was made with “actual malice.”²⁹ Actual malice is having knowledge that a statement is false or exhibiting a reckless disregard for whether the statement is false or not.³⁰

Additionally, the “public figure” constitutional protection extension comes from *Gertz v. Robert Welch, Inc.*³¹ In *Gertz*, the United States Supreme Court stated that the public figure designation arises when a person is a general or limited purpose public figure.³² General-purpose public figures are individuals who have obtained such pervasive fame or notoriety that they become public figures for all purposes and in all contexts. Alternatively, limited-purpose public figures are only public figures for a limited range of issues surrounding a particular public

25. See Bruce P. Smith, *Cybersmearing and the Problem of Anonymous Online Speech*, 18 J. MEDIA, INFO., & COMM. L. 3, 5 (Fall 2000).

26. See *id.* at 7–8.

27. See Jeffrey R. Elkin, *Cybersmears: Dealing With Defamation on the Net*, BUS. L. TODAY, Jan.–Feb. 2000, at 22.

28. 376 U.S. 254 (1964).

29. *Id.* at 279–80.

30. *Id.* at 280.

31. 418 U.S. 323 (1974).

32. *Id.* at 351.

controversy.³³ It is much easier for a defendant to defeat a defamation claim when the plaintiff is a public official or public figure than when the plaintiff is a private individual.³⁴ A judge decides whether a plaintiff is a public official or figure, and each case is fact-specific.³⁵

A new trend appears to be emerging in defamation cases at the lower court level involving anonymous speakers and writers. When faced with defamation lawsuits against anonymous posters, courts seem to be questioning whether these suits are brought for meritorious reasons or merely to unmask the posters, so that they may be silenced or terminated. The chilling effect of defamation suits and the accompanying discovery, which matches real names with pseudonyms, is perhaps the greatest where the plaintiff employs the posters. In addition, even anonymous investors posting messages may seek protection from unmasking pursuant to the theories afforded in late-breaking decisions.

III. ANONYMOUS POSTERS PROTECTED BY ANTI-SLAPP LEGISLATION

In a recent case, *Global Telemedia International, Inc. v. Doe 1*,³⁶ a federal court held that California's Strategic Litigation Against Public Participation ("SLAPP") statute should be applied to anonymous postings on an Internet message board.³⁷ In *Global Telemedia*, the plaintiffs brought suit against numerous John Does, including King and Reader, for posting anonymous negative comments about Global Telemedia International, Inc. ("GTMI") and Jonathan Bentley Stevens, then CEO of GTMI, on an Internet message board.³⁸ The plaintiffs brought multiple actions against the defendants including trade libel, libel per se, and interference with contractual relations.³⁹ The defendants argued that California's statute allowing defendants to dismiss SLAPP suits was applicable to the case.⁴⁰ This was a significant victory for the defendants,

33. See Elkin, *supra* note 27, at 24 (interpreting the language of *Gertz*, 418 U.S. at 351).

34. See generally Michael Hadley, Note, *The Gertz Doctrine and Internet Defamation*, 84 VA. L. REV. 477, 477, 500 n.182 (1998) (discussing the higher standard of actual malice for public figures is "almost impossible" to meet).

35. See Elkin, *supra* note 27, at 24 (citing *WFAA-T.V., Inc. v. McLemore*, 978 S.W.2d 568, 571 (Tex. 1998)).

36. 132 F. Supp. 2d 1261 (C.D. Cal. 2001).

37. *Id.* at 1266. See Cassell Bryan-Low, *Name Games: E*Trade Sues Over Postings*, WALL ST. J., Feb. 28, 2001, at C1 (quoting attorney for the defense, Megan E. Gray, claiming the case "has broad implications" as the ruling extends the contexts in which posting are protected).

38. *Global Telemedia*, 132 F. Supp. 2d at 1263-64.

39. *Id.* at 1264.

40. *Id.* at 1265 (citing CAL. CIV. PROC. CODE § 425.16 (West Supp. 2001)).

one that will likely result in more use of this new legal defense when plaintiff companies bring suit against anonymous Internet message board posters.

California's anti-SLAPP legislation, passed in 1992, was intended to prevent the chilling of the exercise of constitutional rights such as free speech through litigation or forms of harassment through the court system.⁴¹ The *Global Telemedia* case extended the protection of the anti-SLAPP statute to shield anonymous message board posters who criticize public corporations against questionable lawsuits brought by the corporation for alleged defamatory statements. The anti-SLAPP legislation "permits a defendant to dismiss a lawsuit if the alleged bad acts arose from his or her exercise of free speech 'in connection with a public issue' and if the plaintiff cannot show a probability of success on the claims."⁴²

In the suit brought by GTMI and others, the plaintiffs did not contest that the defendants were exercising their rights of free speech when posting the negative comments or that the Internet message board was a public forum.⁴³ Instead, plaintiffs argued that the defendants engaged in defamatory commercial speech that was not of public interest.⁴⁴ The United States District Court, however, held that the plaintiff's interpretation of the anti-SLAPP statute was too narrow. The court found that the anti-SLAPP provision protected even commercial speech and recognized it as a form of free speech.⁴⁵ The *Global Telemedia* Court noted, however, that precedent established in *Globetrotter Software, Inc. v. Elan Computer Group* prevented a business competitor from using the anti-SLAPP statute to protect commercial speech.⁴⁶ But because neither defendant was a business competitor of the plaintiffs, the postings were viewed by the court as an exercise of the defendants' right of free speech, albeit commercial in nature.⁴⁷

The *Global Telemedia* Court interpreted Section 425.16 of the California Code of Civil Procedure not only to require comments to be an exercise of the defendants' right of free speech, but also to connect the comments with a public issue.⁴⁸ The court found that GTMI was of public interest because it is a publicly traded company with 18,000 investors,

41. *Id.* at 1264-65.

42. *Id.* at 1265 (quoting CAL. CIV. PROC. CODE § 425.16(b)(1) (West Supp. 2001)).

43. *Id.* at 1265.

44. *Id.*

45. *Id.* at 1265-66.

46. *Id.* (citing *Globetrotter Software, Inc. v. Elan Computer Group*, 63 F. Supp. 2d 1127, 1130 (N.D. Cal. 1999)).

47. *Id.* at 1266.

48. *Id.* at 1265.

it uses the media to distribute good news about the company to be attractive to investors, and GTMI has been the target of more than 30,000 Internet postings.⁴⁹

The court essentially extended anti-SLAPP protection to cyberspace and anonymous Internet posters by ruling that the defendants satisfied the free speech and public concern requirements of the anti-SLAPP statute.⁵⁰ The *Global Telemedia* ruling will likely have a significant impact on these "cyber-SLAPP" cases because twelve other states, in addition to California, have anti-SLAPP laws, including Colorado, Delaware, Georgia, Maine, Massachusetts, Minnesota, Nebraska, New York, Oklahoma, Rhode Island, and Tennessee.⁵¹ Ten other states have been reportedly contemplating anti-SLAPP legislation.⁵²

It should be noted that California Code of Civil Procedure § 425.16 still provides the plaintiff the opportunity to overcome an anti-SLAPP defense if it is able to demonstrate a probability of success.⁵³ In the *Global Telemedia* case, the plaintiffs could not convince the court that they would likely prevail on their claims against the defendants.⁵⁴ The court found that the defamation actions against the defendants would be unsuccessful because the postings were opinions rather than facts, and that even if the comments were found to be factual, the plaintiffs suffered no harm by the defendants' comments.⁵⁵

In *Global Telemedia*, the defendants were able to apply California's anti-SLAPP legislation to successfully defend against GTMI's numerous causes of action. The court granted a motion to dismiss prior to discovery of the identities of the posters, thus defeating the plaintiff's lawsuit, and thereby preventing what has become a common method for corporations to expose and silence anonymous critics on Internet message boards.⁵⁶

IV. CONSTITUTIONAL PROTECTION OF ANONYMOUS SPEECH

First Amendment protection for public speech made by anonymous persons was explicitly recognized by the United States Supreme Court in *McIntyre v. Ohio Elections Commission*.⁵⁷ The *McIntyre* Court ruled that

49. *Id.*

50. *Id.* at 1265–66.

51. See Lidsky, *supra* note 6, at 945 n.506.

52. *Id.*

53. *Global Telemedia*, 132 F. Supp. 2d at 1266.

54. *Id.* at 1270–71.

55. *Id.* at 1267–70.

56. See *id.* at 1270–71.

57. 514 U.S. 334 (1995).

anonymous opinion about public issues or concerns is protected speech under the First Amendment.⁵⁸ The *McIntyre* case involved an action by the deceased pamphleteer's executor, Joseph McIntyre, who continued to pursue the matter upon the death of pamphleteer Margaret McIntyre.⁵⁹ Mr. McIntyre challenged the fine imposed on Ms. McIntyre by the Ohio Elections Commission for distributing anonymous leaflets opposing a proposed school tax levy.⁶⁰

The question presented in *McIntyre* was whether an Ohio statute that prohibited the distribution of anonymous campaign literature abridged an individual's freedom of speech within the meaning of the First Amendment.⁶¹ The Court held that "the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment."⁶² Referring to literary works, the Court stated that "[t]he decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."⁶³ The Court, however, citing *Talley v. California*,⁶⁴ stated that "[t]he freedom to publish anonymously extends beyond the literary realm. In *Talley*, the Court held that the First Amendment protects the distribution of unsigned handbills urging readers to boycott certain Los Angeles merchants who were allegedly engaging in discriminatory employment practices."⁶⁵

The *Talley* Court rejected the argument that a similar ordinance was "aimed at providing a way to identify those responsible for fraud, false advertising and libel"⁶⁶ because "nothing in the text or legislative history of the ordinance limited its application to those evils."⁶⁷ Likewise in *McIntyre*, the state statute contained no language limiting its application to fraudulent, false or libelous statements. Therefore, to the extent that Ohio sought to justify its statute "as a means to prevent the dissemination of untruths, its defense . . . [failed] for the same reason given in *Talley*."⁶⁸

Nevertheless, the *McIntyre* Court distinguished the statute in *Talley* from the Ohio statute because the Ohio statute applied only to unsigned

58. *Id.* at 357.

59. *Id.* at 340.

60. *Id.* at 337-38.

61. *Id.* at 336.

62. *Id.* at 341.

63. *Id.* at 341-42.

64. 362 U.S. 60 (1960).

65. *McIntyre*, 514 U.S. at 342.

66. *Id.* at 343 (quoting *Talley*, 362 U.S. at 64).

67. *Id.*

68. *Id.* at 344.

documents designed to influence voters in an election, while the Los Angeles statute at issue in *Talley* “prohibited all anonymous handbilling ‘in any place under any circumstances.’”⁶⁹ The *McIntyre* Court held that the Ohio statutory prohibition against the distribution of anonymous campaign literature violated the First Amendment.⁷⁰ The Court declared that the State “cannot seek to punish fraud indirectly by indiscriminately outlawing a category of speech, based on its content, with no necessary relationship to the danger sought to be prevented.”⁷¹

V. PRIVATE SECTOR EMPLOYEE RIGHTS TO POST ANONYMOUSLY

It is clear that First Amendment free speech rights protect against government action.⁷² But what of private employer action or reaction to anonymous postings where the posters turn out to be employees? What free speech rights do private sector employees have? Are private sector employers restricted from silencing their employees by the federal Constitution in the same manner as public sector employers?⁷³ The rights of private sector employees to speak their minds, even on their own time, and on their own computers, may be noticeably chilled by fear of employer retaliation.

For the most part, employers in the private sector retain the power to hire, fire, and discipline employees in accordance with the employer’s legitimate business interest. One such interest is an employer’s interest in protecting its reputation. Even where a matter may be of public concern, and about a company that has sought the media to enhance its image, that company may wish to discover the disseminator of statements that cast it in an unfavorable light. Employees are perhaps more likely to have and express such opinions about their employer than about other companies with which they are far less familiar. Examining these competing interests, several questions arise. If employees express their opinions online about publicly disclosed information, is this an offense

69. *Id.* (quoting *Talley*, 362 U.S. at 60–61).

70. *Id.* at 357.

71. *Id.*

72. See LAWRENCE LESSIG, CODE & OTHER LAWS OF CYBERSPACE 164 (1999).

73. See DAVID P. TWOMEY, LABOR & EMPLOYMENT LAW 614–15 (11th ed. 2001) (citing *K-Mart Corp. v. Trott*, 677 S.W.2d 632 (Tex. Civ. App. 1984). See also *Watchtower Bible and Tract Society, Inc. v. Stratton*, 240 F.3d 553 (6th Cir. 2001) *cert. granted*, 122 S.Ct. 392 (2001). The Supreme Court heard oral arguments on Feb. 26, 2002 in this case. The Court is considering the level of protection that is due for anonymous nonpolitical speech—in this case speech of a religious nature—and whether this speech deserves the same high level of protection that anonymous political speech enjoys, as established by the *McIntyre* decision. 514 U.S. 334, 336 (1995). The decision in *Watchtower* thus will impact speech of an anonymous nonpolitical nature, such as that considered in cybersmear cases.

for which they may be disciplined or discharged?⁷⁴ Or does the opinion privilege of the First Amendment protect derogatory employee posters? Should the courts look at private sector employee postings differently in light of the constraints placed upon employees within the employment relationship?⁷⁵

The use of technology itself to disseminate messages poses other difficult issues courts may need to resolve on the way to resolving the previous questions. Should computer postings be treated differently than the more traditional avenues of expression afforded by newspapers, newsletters, or handbills? Should the greater reach of language in cyberspace result in equating such publications with radio or television broadcast? To the extent that Internet bulletin boards are loose forums where posters may aim to inflame the audience and proudly strut unfounded opinions, the context is unlike ordinary communication media. So long as anonymity reigns, an employee poster suffers no harm for his or her derogatory postings regarding the employer. But if a plaintiff employer establishes a probability of success on the merits of its defamation claim and discovers the poster's identity, where will the private sector employee look for protection? Perhaps the employee might look for guidance to the common law public policy and explicit statutory protections afforded employee speech in other situations. The regulatory environment of employment sets some boundaries in other contexts that may apply to employee posters as well.

Employees have a federal right to engage in "concerted activity" within the meaning of Section 7 of the National Labor Relations Act⁷⁶ and this protection applies whether or not the employees are unionized.⁷⁷

74. It is a completely different matter if an employee discloses private proprietary information, trade secrets, or breaches a duty of confidentiality in violation of an employment agreement while discussing company activities online. These cases do not compare with an employee writing about publicly disclosed information and/or to instances where there is no violation of an express employment agreement. Beyond contractual prohibitions, one might also consider an agent's duties of loyalty, good faith, and the duty to inform the principal of all relevant information, etc., to the extent that such duties apply in an employment context where the employer is the principal and the employee is the agent. *See Immunomedics, Inc. v. Jean Doe*, 775 A.2d 773, 777-78 (N.J. Super. Ct. App. Div. 2001) ("Individuals choosing to harm another or violate an agreement through speech on the Internet cannot hope to shield their identity and avoid punishment through invocation of the First Amendment.").

75. *See TWOMEY*, *supra* note 73, at 623 (noting that employers may monitor employee e-mail under the Electronic Communication Privacy Act); *see also* Michael J. McCarthy, *Web-surfers Beware: The Company Tech May be a Secret Agent*, WALL ST. J., Jan. 10, 2000, at A1 (discussing the ease with which a company may monitor its employees' Internet traffic).

76. 29 U.S.C. § 157 (1994).

77. Section 7 of the National Labor Relations Act provides in pertinent part:

Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining

Even with this right, however, employers retain the ability to limit employee speech that interferes with work activity during working hours, as long as “concerted activity” speech is not limited any more than other forms of speech that interfere with work and occur during working hours.⁷⁸ Employer rules regulating speech must not discriminate against employees who choose to form or to join a union, or who engage in discussion for mutual aid and protection, lest the employer run afoul of statutory protections afforded to employees.

Other areas where employer regulation of employee speech may conflict with employee rights include interference with such protected activities as whistleblowing.⁷⁹ Employees may be anxious to discuss perceived serious safety conditions or illegal activities. But once again, is posting such information on a computer bulletin board the appropriate route for seeking its correction? Still, further issues arise regarding employee postings that relate to religion, gender, disability, sexual orientation, etc. To the extent that both federal and state laws protect employees from discrimination on these bases, employers who allow online harassment of its employees by other employees may be held liable for their failure to intervene.⁸⁰

or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities

29 U.S.C. § 157 (1994). However, the supervisory and managerial employees are not included within the protections afforded employees by the National Labor Relations Act. *See* National Labor Relations Act, 29 U.S.C. §§ 151–69 (1994); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974).

78. It is an unfair labor practice for an employer to set different, more restrictive standards for policing “concerted activity” than other non-productive or non-work activity. This amounts to discrimination on the basis of a protected activity. *See* 29 U.S.C. § 158 (a)(3) (1994). Rules similar to those applied in the concerted activity context in traditional modes of communication should apply in cyberspace. As scholars have noted, “[d]enial of access to electronic communication networks . . . will likely work a greater interference with employees’ rights to engage in concerted activities than will denial of access to a workplace’s physical plant.” Martin H. Malin & Henry H. Perritt, Jr., *The National Labor Relations Act in Cyberspace: Union Organizing in Electronic Workplaces*, 49 U. KAN. L. REV. 1, 63 (2000).

79. *See* Elletta Sangrey Callahan & Terry Morehead Dworkin, *The State of State Whistleblower Protection*, 38 AM. BUS. L.J. 99, 100, 130 (2000) (discussing whistleblowing exception to the doctrine of employment at will and noting the enactment of whistleblower protection statutes in fifty states).

80. *See* Mark E. Schreiber, *Employer E-Mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 76–77 (2000) (noting employer liability for improper or offensive e-mail or web traffic in race and sexual harassment cases); *See also* Gerald L. Maatman, Jr., *Cyberspace Harassment*, 2 J. EMP. DISCRIMINATION. L. 286, 287–88 (2000) (discussing employer liability for e-mail postings on Internet bulletin board constituting workplace sexual harassment where employer failed to remedy); *cf.* Schreiber, *supra*, at 80 (stating that federal law restricts employer liability for defamation to cases where “the employee acts within the scope of his employment and the employer either had knowledge of, ratified, or recklessly disregarded such conduct.”).

Employees may have protection to voice their opinions between each other regarding numerous matters, but their rights must be balanced against the needs of others, both within the workplace and outside of it. In the cyber era, managers retain significant managerial prerogative to limit employee speech. Errant speech may prove costly to employees if employers succeed in unmasking them as anonymous posters. While the right to speak anonymously is constitutionally protected, that protection is not without limits. The laws of defamation remain available to pursue employees who post false statements of fact about the company or its principals. Even if the company is a "public" concern or the managers are "public figures," there may well be a basis for a court to find that such facts were posted with "actual malice" or "reckless disregard for truth or falsity." There may also be a basis in contract and tort to discipline or discharge employees, and to seek monetary damages and an injunction against further postings. This could occur where online postings breach confidentiality or restrictive employment covenants, or where the postings divulge trade secrets or otherwise violate what constitutes a well-recognized fiduciary or agency duty to the employer.

VI. HOW THE INTERNET CHANGES THE RULES

Several John Doe cases have been filed recently, corresponding to an increase in anonymous and pseudonymous participation in Internet chat rooms.⁸¹ This phenomenon is due to the attributes and architecture of the Internet. Available at little or no cost, with instant access to an audience of unprecedented reach, and without any sponsor or filter to evaluate the content of posters' speech, the Internet is the most powerful communications medium ever. Employees' speech, which previously had a relatively limited effect on employers, now has the potential scope and impact of a broadcast on the evening news, and then some.

An interesting point to consider in these cases is the juxtaposition of the parties.⁸² Prior to the advent of the Internet as a medium of communication, publishers were invariably large organizational entities. While it is publishers who are still being sued for libel, it is no longer necessarily the *New York Times*, *Hustler* or the *National Enquirer*, to name just a

81. See Carl Kaplan, *Virginia Court's Decision in Online 'John Doe' Case Hailed by Free-Speech Advocates*, N.Y. TIMES ON THE WEB, Mar. 16, 2001, available at <http://courses.cs.vt.edu/~cs3064/lib/Freedom.of.Speech/Anonymous.html> (last visited Aug. 31, 2001) (citing experts' estimate that more than 120 companies have filed Doe suits); Anne Colden, *Sending a Message, Companies Go to Court to Stop 'Cyber-Smeared'*, DENV. POST, Jan. 15, 2001, at E-01 (citing the increase in such suits and estimating that the filings exceed 100 in number).

82. See Lidsky, *supra* note 6, at 893-95.

few well-known libel defendants. Now, one anonymous and pseudonymous individual, because of the Internet, has nearly the same publishing power that a large organization possesses. And the typical plaintiffs in Internet libel cases are now the large organizations. This role reversal changes the nature of the discussion, and suggests that perhaps the historical paradigms of libel and speech are not entirely applicable to cyberspace.

A. *Freedom Fighters or Verbal Terrorists*

Because publishing has never been easier, cheaper, or more targeted, disgruntled posters' messages have found an audience. Employees maintain that they are just expressing their opinion, even the most audacious of which is protected by the First Amendment; that the First Amendment protects anonymous speech; and that anonymous speech fosters free expression. Employers counter that these employees are not freedom fighters, but rather, verbal terrorists who irresponsibly and frivolously defame and libel employers and then hide behind the veil of anonymity and the perceived protections of the First Amendment.⁸³ But the First Amendment, employers point out, does not protect libelous speech.⁸⁴

The shroud of anonymity combined with the qualitatively different manner of expression prevalent on the Internet is the great divider between online and offline libel cases. For all of the value in the constitutional protection of anonymous speech,⁸⁵ it must, nevertheless, be acknowledged that anonymity has the potential to conceal illegal activity.⁸⁶ Therefore, an individual may not extend the protection of his or her speech under the First Amendment to violations of the law simply by choosing to remain anonymous.⁸⁷ It is imperative, however, that employer suits attempting to strip employees of their anonymity are most carefully evaluated. How then do courts address these important issues in the context of pre-litigation subpoena cases?

83. See Lidsky, *supra* note 6, at 945 (concluding that "many plaintiffs will have legitimate claims against aggressively uncivil and vicious speakers whose only intent is to destroy the reputation of their targets.").

84. See *Beauharnais v. Illinois*, 343 U.S. 250, 266 (1952) (holding that libelous statements are outside the realm of constitutionally protected speech).

85. See *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 341-42, 357 (1995).

86. See *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) ("With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information.").

87. *Id.* ("People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law." [emphasis added]).

B. Balancing the Equities: Employer Redress, Employee Speech and the Necessity of Disclosure—Developing a Standard

In John Doe defamation cases courts must decide whether to order the identification of an anonymous Internet poster against whom an action has been filed, or to allow the individual to remain anonymous. Courts must discern whether the plaintiff has supportable claims and whether the law supports immunity for the posters. Moreover, all of this has to be accomplished even before the complaint has been served and litigation truly begins. The tension involved in cybersmear lawsuits between anonymity and accountability has analogies in privacy and First Amendment jurisprudence, and of course in anti-SLAPP litigation.⁸⁸ Courts have recognized a qualified privilege against disclosure in cases where disclosure would harm the exercise of a fundamental right.⁸⁹ How courts have resolved these matters in such contexts is instructive with regard to John Doe cybersmear suits.

Two approaches to pre-subpoena litigation have developed in court decisions beginning in 2000. The first court to issue an opinion on this issue was a Virginia state court, in *In re Subpoena Duces Tecum To America Online, Inc.*⁹⁰ The court considered the issue in the context of an ISP challenging a plaintiff's attempts to unmask anonymous posters who subscribed to AOL's service. AOL moved to quash a subpoena issued in support of plaintiff's discovery.⁹¹ Plaintiff, an anonymous publicly traded company ("APTC"), wished to ascertain who was posting allegedly defamatory material misrepresentations and confidential information about its company. AOL responded that it was unwilling to voluntarily comply with the subpoena. The court framed the issue as follows:

As this Court has determined that the subpoena can have an oppressive effect on AOL, the sole question remaining is whether the subject subpoena is unreasonable in light of all the surrounding circumstances. Ultimately, this Court's ruling . . . must be governed by a determination of whether the issuance of the subpoena duces tecum and the potential loss of the anonymity of the John Does, would constitute an unreasonable intrusion on their First Amendment rights. In broader terms, the issue can be framed as whether a state's interest in protecting its citizens

88. See *Global Telemedia Intern., Inc. v. Doe 1*, 132 F. Supp. 2d 1261, 1264-66 (C.D. Cal. 2001).

89. See *Bates v. City of Little Rock*, 361 U.S. 516 (1960); *NAACP v. Alabama*, 357 U.S. 449 (1958).

90. 52 Va. Cir. 26 (Va. Cir. Ct. 2000), *rev'd on other grounds sub nom. America Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

91. *Id.* at 27.

against potentially actionable communications on the Internet is sufficient to outweigh the right to anonymously speak on this ever-expanding medium. There appear to be no published opinions addressing this issue either in the Commonwealth of Virginia or any of its sister states.⁹²

AOL proposed that the Court adopt a two-prong test to determine when a subpoena request is reasonable and would require it to identify its subscribers: (1) the plaintiff must plead with specificity a prima facie claim that it is the victim of recognized tortious conduct and (2) the subpoenaed information must be centrally needed to advance that claim.⁹³ Finding AOL's proposed test "too cumbersome" (in that courts would be asked to determine the sufficiency of pleadings, which vary from state to state), the Court instead created this rule:

when a subpoena is challenged . . . , a court should only order . . . [an ISP] to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of [actionable] conduct . . . and (3) the subpoenaed identity information is centrally needed to advance that claim.⁹⁴

The Court denied AOL's motion to quash, finding that under its new test, all three prongs had been satisfied as to the identities of the AOL subscribers. The anonymous posters were ordered unmasked. The court found that the "compelling state interest in protecting companies such as APTC from the potentially severe consequences that could easily flow from actionable communications . . . significantly outweigh the limited intrusion on the First Amendment rights of any innocent subscribers."⁹⁵

Also in 2000, a New Jersey state trial court heard the *Dendrite*⁹⁶ case. This case arose in the context of anonymous posters themselves challenging plaintiff's attempts to unmask them. Acknowledging the Virginia state court's decision in *AOL*, as well as the Northern District of California's opinion in *Columbia Ins. Co. v. Seescandy.com*,⁹⁷ a federal trademark case, the court adopted the approach taken by the latter

92. *Id.* at 33 (footnote omitted).

93. *Id.* at 36.

94. *Id.* at 37.

95. *Id.* at 37.

96. *Dendrite Int'l, Inc. v. John Does*, No. MRS C-129-00, (N.J. Super. Ct. Ch. Div., Nov. 23, 2000) available at <http://www.citizen.org/documents/dendrite.pdf> (last visited Jan. 21, 2002), *aff'd*, 775 A.2d 756 (N.J. Super. Ct. App. Div., 2001).

97. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

court.⁹⁸ *Seescandy.com* arose in a different context, a domain name dispute. Nevertheless, the case involved a plaintiff seeking to unmask anonymous defendants prior to service of process. That court was asked to grant a temporary restraining order ("TRO") without knowing the identity of the defendant whom plaintiff had not yet located.⁹⁹ The court's ruling focused solely on the procedural propriety of allowing pre-service discovery. The court considered whether it should authorize discovery to establish the defendants' identities sufficiently such that they could be served with process,¹⁰⁰ noting that:

[a]s a general rule, discovery proceedings take place only after the defendant has been served; however, in rare cases, courts have made exceptions, permitting limited discovery to ensue after filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant.¹⁰¹

Specifically in reference to anonymous online speech, the court added:

People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. . . . 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.¹⁰²

Mindful that the traditional reluctance to permit Doe filings (because they do not comply with service requirements) must be tempered by the need to provide injured parties with a forum, the *Seescandy.com* Court enunciated a four-prong test to determine whether discovery to uncover the identity of a defendant is warranted. First, the plaintiff must identify the defendant with sufficient specificity. Second, the plaintiff must identify all previous steps taken to locate the defendant (thus evidencing a good faith effort to comply with service of process requirements). Third, the plaintiff must establish that its suit can withstand a motion to dismiss. Fourth, the plaintiff must file a request for discovery, along with a statement of justifications for this request, as well as the 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 this

98. *Dendrite I*, *supra* note 96, at 6-7.

99. *Seescandy.com*, 185 F.R.D. at 575.

100. *Id.* at 577.

101. *Id.* (citations omitted).

102. *Id.* at 578.

discovery will lead to identifying information that would make service of process possible.¹⁰³

The *Dendrite* Court, citing New Jersey's commitment to maintaining the anonymity of individuals in specific situations, adopted the test of *Seescandy.com* and required Dendrite International to satisfy it "before the Court will impinge upon a defendant's Constitutional Right to Free Speech."¹⁰⁴ This first *Dendrite* opinion, issued November 23, 2000, is a landmark decision on the rights of individuals to communicate anonymously and pseudonymously on the Internet about matters of public concern.¹⁰⁵ (The court did not issue a decision with regard to John Does 1 and 2, as they did not respond in this case. Because of this, the court granted Dendrite's request as to those two defendants.)¹⁰⁶ John Does 3 and 4 engaged counsel immediately to challenge Dendrite's efforts to unmask them. As to these defendants, the court refused to grant Dendrite's pre-service subpoena motion.¹⁰⁷ Significantly, the court imposed a burden of proof higher than that usually required for a motion to dismiss. Because of this more searching review, the court found that Dendrite did not make out a prima facie case of defamation against John Doe 3. Further, the court found that the company failed to provide the Court with "ample proof from which to conclude that John Does Nos. 3 and 4 have used their constitutional protections in order to conduct themselves in a manner which is unlawful or that would warrant this Court to revoke their constitutional protections."¹⁰⁸ Dendrite appealed the decision to the Superior Court of New Jersey.

On review, a three-judge panel considered Dendrite's contention that the court should compel identity disclosure.¹⁰⁹ The court noted that the present case focused on John Doe No. 3's comments as the basis for Dendrite's defamation claims.¹¹⁰ Reviewing the *Seescandy.com* approach,

103. *Id.* at 578–80.

104. *Dendrite Int'l, Inc. v. John Does, No. MRS C-129-00*, at 8 (N.J. Super. Ct. Ch. Div., Nov. 23, 2000) available at <http://www.citizen.org/documents/dendrite.pdf> (last visited Jan. 21, 2002), *aff'd*, 775 A.2d 756 (N.J. Super. Ct. App. Div., 2001).

105. See Mary P. Gallagher, *Cybersmeared Defendants Can Keep Anonymity by Appearing in Court: Ruling Breaks New Ground in Litigation over Online Defamation*, N.J.L.J., Dec. 4, 2000, at 7 (reporting that this was a case of first impression, and noting Paul Levy's comments that this "decision marks the first time that a judge has rejected a request for identification"). See generally Saitz, *supra* note 5 (reporting that this state court decision was "only the second time in the country in which a judge sided with unnamed message posters after balancing their constitutional rights against the merits of a defamation suit").

106. *Dendrite I*, *supra* note 104, at 22.

107. *Id.*

108. *Id.*

109. *Dendrite Int'l Inc. v. John Doe 3*, 775 A.2d 756, 759–60 (N.J. Super. Ct. App. Div., 2001).

110. *Id.* at 760.

the appellate court affirmed the analysis, with some refinements.¹¹¹ The essential issue on appeal related to the third prong of analysis, wherein plaintiff must establish that its suit could withstand a motion to dismiss.¹¹² Dendrite alleged on appeal that it did just that, and that the lower court substituted a higher, more searching standard in this regard, in contravention of recognized standards for motions to dismiss.¹¹³ The lower court found, under this more exacting standard, that Dendrite failed to show that the statements posted by John Doe No. 3 caused any harm to Dendrite.¹¹⁴ However, the Dendrite complaint would withstand a motion to dismiss under the normal, less-exacting standard.

Finding that the lower court did indeed require more "evidentiary support for the pleading than is traditionally required when applying motion-to-dismiss standards,"¹¹⁵ the appellate court nevertheless affirmed the decision. The court reasoned that this easy-to-meet "standard in isolation fails to provide a basis for analysis and balancing of Dendrite's request for disclosure in light of John Doe No. 3's competing right of anonymity in the exercise of his right to free speech."¹¹⁶ The Superior Court agreed that such use of the judicial process, in relation to the important rights involved, necessitated reliance on a higher standard analogous to the probable cause standard used in criminal investigations.¹¹⁷ In effect, the probable cause standard required Dendrite to "make some showing that an act giving rise to civil liability actually occurred and that the discovery is aimed at revealing specific identifying features of the person or entity who committed the act."¹¹⁸

Along with its reliance on *Seescandy.com*, the court found support for its more exacting standard in *In re Subpoena Duces Tecum To America Online, Inc.*¹¹⁹ Applying this higher standard to the case of John Doe No. 3, the *Dendrite* court affirmed the denial of Dendrite's motion. The court concluded that Dendrite failed to demonstrate that Doe No. 3's postings caused any harm.¹²⁰ A review of the testimony, trading history of

111. *Id.* at 760-61.

112. *Id.* at 766.

113. *Id.*

114. *Id.*

115. *Id.* at 769.

116. *Id.* at 770.

117. *Id.*

118. *Id.* (quoting *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 580 (N.D. Cal. 1999)).

119. 52 Va. Cir. 26 (Va. Cir. Ct. 2000), *rev'd on other grounds sub nom. America Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

120. *Dendrite II*, 775 A.2d at 771-72.

Dendrite shares, and other news failed to reveal a connection between John Doe No. 3's actions and any harm to Dendrite International.¹²¹

The Superior Court enunciated the following test to determine if, and when, to compel identity disclosure. The trial court must: (1) require plaintiff to first undertake efforts to notify the anonymous posters that they are the subject of a subpoena; (2) require plaintiff to identify and set forth the exact statements purportedly made by the anonymous posters that allegedly constitute actionable speech.¹²² Thus, plaintiff must set forth a prima facie cause of action (which is a more demanding standard than that generally required for a complaint). Finally, (3) assuming there is a prima facie cause of action, the court must balance the defendant's First Amendment rights of anonymous free speech against the strength of plaintiff's case *and* the necessity for the disclosure of defendant's identity (so as to allow plaintiff to properly proceed).¹²³

The New Jersey Superior Court opinion provides much needed guidance in a new area of law. The court artfully navigated the many explosive issues and compelling needs of the parties and calibrated their relative rights and responsibilities. John Doe No. 3 prevailed in the case. Interestingly, the court took action on a similar case the same day, with an opposite outcome.

Plaintiffs prevailed in the companion case, *Immunomedics, Inc. v. Jean Doe*.¹²⁴ This case arose in the context of a defendant employee who breached a confidentiality agreement with her employer through anonymous postings.¹²⁵ The plaintiff employer sought to compel identity disclosure. Applying the same analytical framework as in *Dendrite*, the court in this instance affirmed identity disclosure of the anonymous poster.¹²⁶ The difference in *Immunomedics* was that the company met all conditions under the three-part test, so the court struck the balance in favor of disclosure.¹²⁷ The evidence demonstrated the poster was an employee, that she executed a confidentiality agreement, and that the contents of the messages provided evidence of a breach of the agreement.¹²⁸ The court warned that although anonymous speech is protected, there must be an avenue of redress for those who are wronged.¹²⁹ Individuals cannot avoid punishment through invocation of the First

121. *Id.* at 772.

122. *Id.* at 760.

123. *Id.* at 760–61.

124. 775 A.2d 773 (N.J. Super. Ct. App. Div., 2001).

125. *Id.* at 774.

126. *Id.* at 777–78.

127. *Id.*

128. *Id.* at 777.

129. *Id.* at 777–78.

Amendment.¹³⁰ The contrasting outcomes of *Dendrite* and *Immunomedics* are instructive for sorting out identity disclosure claims in the future. These cases represent an excellent foundation for the developing jurisprudence of compelling identity disclosure of anonymous posters through pre-subpoena discovery and litigation.

CONCLUSION

This is indeed a wide-open area of state law. As a result, it is almost impossible to establish a consistent framework of analysis for anonymous Internet speech cases. A patchwork of differing standards by which to judge these cases undercuts one of the cardinal values of the law—predictability.

Anonymous and pseudonymous individuals—actually, all individuals have a reasonable expectation of privacy and a right to speak anonymously. Speech and privacy are fragile, especially in instances when the speech concerns terms of employment or working conditions. No rights are granted without limitation, however, and speech and privacy are no exceptions. These rights must be protected, but those who commit defamation must also be accountable for their actions. The law is rapidly developing with regard to cybersmear and cyber-SLAPP litigation in which plaintiffs are invoking the power of the legal system to compel identification of anonymous posters.

As the Public Citizen Litigation Group states, courts must “develop a test for the identification of anonymous posters which neither makes it too easy for vicious defamers to hide behind pseudonyms, nor makes it too easy for a big company to unmask its critics by the simple device of filing a complaint which manages to state a valid claim for relief under some tort or contract theory.”¹³¹

The four-part test that Judge MacKenzie adopted in the *Dendrite* decision, as refined by the Superior Court, goes a long way toward achieving this balance between employees’ speech and privacy rights, employers’ reputational interests, and the necessity of compelling identity disclosure.

130. *Id.* at 778.

131. Brief of Amici Curiae Public Citizen and the ACLU of New Jersey at Argument, Section C Part 2, *Dendrite International, Inc v. Doe No. 3*, 775 A.2d 756 (N.J. Super. Ct. App. Div., 2001) (No. A-2774-00) at <http://www.citizen.org/litigation/briefs/1stAmendment/articles.cfm?ID=1862> (last visited Feb. 1, 2001).