THE YALE LAW JOURNAL

NATHANIEL GLEICHER

John Doe Subpoenas: Toward a Consistent Legal Standard

ABSTRACT. This Note considers the rising trend of anonymous online harassment and the use of John Doe subpoenas to unmask anonymous speakers. Although anonymity often serves as an important shield for valuable speech, it also protects online harassment that can chill or completely silence the speech of its targets. This Note argues that the public figure doctrine should be adapted to John Doe subpoenas to distinguish between online harassment and more valued anonymous speech. It then divides John Doe subpoena standards into six constituent factors, evaluates each one, and proposes a final standard that consistently balances the needs of plaintiffs and defendants and helps judges to distinguish online harassment from other forms of anonymous speech.

AUTHOR. Yale Law School, J.D. 2009; University of Chicago, B.S. 2003. I am especially grateful to Professor Jack Balkin for his guidance and advice in developing this piece, and to Professor Danielle Citron for her extensive comments and edits. I am also indebted to Professor Robert Post for his helpful comments on composing my standard. Thanks also to Kyle Glover, Brittan Heller, and my family for their advice and unwavering support.

NOTE CONTENTS

INTRODUCTION 323

I. WHAT IS A JOHN DOE SUBPOENA? 326
- A. The Qualified Privilege of Anonymous Speech 326
- B. From John Doe Pleading to John Doe Subpoenas 327
- C. The Unique Features of John Doe Subpoenas 329

II. DISTINGUISHING ONLINE HARASSMENT FROM TRADITIONAL ANONYMOUS ONLINE SPEECH 330
- A. Public Figure Doctrine 332
- B. Adapting the Public Figure Standard to Anonymous Online Speech 334
- C. Distinguishing Between Chilling and Nonchilling Speech 336

III. EVALUATING THE CURRENT STANDARDS AND DEVELOPING A SINGLE BALANCED STANDARD 337
- A. Existing John Doe Subpoena Standards 338
- B. Notice and Opportunity To Respond 345
  1. Who Should Be Required To Notify? 345
  2. How Should the Defendant Be Notified? 347
  3. How Long Should the Defendant Have To Respond? 349
  4. An Appropriate Standard for Defendant Notice 350
- C. Strength of Plaintiff's Argument 350
  1. Good Faith 350
  2. Survive a Motion To Dismiss 351
  3. Withstand a Motion for Summary Judgment 352
  4. Establish a Prima Facie Case 353
  5. The Problem of Elements that Are Beyond the Plaintiff's Control 354
  6. Heightened Standard for Public Figure Plaintiffs 355
  7. An Appropriate Standard for the Strength of the Plaintiff's Argument 357
- D. Relevance of Information Sought 357
- E. Specificity of Crime and Evidence 359
- F. Balancing the Rights of the Plaintiff and the Defendant 360
- G. Exhaustion of Alternatives 362

IV. A SINGLE STANDARD FOR JOHN DOE SUBPOENAS 362
A. Identifying an Anonymous Defendant 363
B. Applying the Standard: AutoAdmit 364

CONCLUSION 368

INTRODUCTION

Anonymous speech conjures the image of a pamphleteer who speaks out against corruption, defying the voices of power and publishing anonymously for fear of reprisal. Two centuries ago, pamphleteers worked on printing machines, distributing their words by pony express and stagecoach. Our Founding Fathers debated the makeup of the fledgling United States under pseudonyms.[1] Today, anonymous speakers use blogs, message boards, and online wikis to reach millions of readers. In these new media, which are virtually free of production and delivery costs, anyone can become a modern-day muckraker, exposing scandal and speaking out against fraud from the safety of his or her computer. From anonymous message boards criticizing massive corporations,[2] to citizens who scrutinize elected officials,[3] to websites that enable the anonymous release of government and corporate documents,[4] the Internet has expanded the cape of anonymity to shield an army of pamphleteers.

The Internet can keep speakers anonymous, but it can also thrust unsuspecting subjects into the harsh eye of the public. A high school boy who videotaped himself imitating a Jedi, with a golf club in place of a lightsaber, became an international sensation when other students posted his video on YouTube. It quickly became one of the most watched videos on the Internet, spawning a legion of imitations and mashups. The teasing—at school, around town, and online—was merciless.[5] The megaphone of the Internet does not merely magnify socially conscious speech. It also lends casual bullying a global

1. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 n.6 (1995) (describing Publius, the pen name under which Alexander Hamilton, John Jay, and James Madison wrote *The Federalist Papers*).

2. *See, e.g.*, ComCraptic.com - Your Chance To Tell Everyone How You Feel About Comcast Products and Service, http://comcraptic.com (last visited Oct. 27, 2008); DeltaReallySucks.com, http://deltareallysucks.com (last visited Oct. 27, 2008).

3. *See, e.g.*, Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005) (rejecting a city councilman's attempt to unmask an anonymous critic).

4. *See, e.g.*, Jonathan D. Glater, *Judge Reverses His Order Disabling Web Site*, N.Y. TIMES, Mar. 1, 2008, at A11; Adam Liptak & Brad Stone, *Judge Shuts Down Web Site Specializing in Leaks, Raising Constitutional Issues*, N.Y. TIMES, Feb. 20, 2008, at A14.

5. *See Star Wars Kid Is Top Viral Video*, BBC NEWS, Nov. 27, 2006, http://news.bbc.co.uk/1/hi/entertainment/6187554.stm; Tu Thanh Ha, *'Star Wars Kid' Cuts a Deal with His Tormentors*, GLOBE & MAIL (Toronto), Apr. 7, 2006, at A8.

reach.[6] New technology has made harassment more possible and powerful online even as it has empowered modern-day pamphleteers to speak anonymously to ever-growing audiences.

Combining these two phenomena reveals the dark side of anonymous online speech. Anonymity increasingly serves as a cover for gossip, defamation, harassment, and even assault on the Internet. Faceless crowds of online tormentors wield virtual pitchforks, carry virtual torches, and hound innocent targets into hiding and out of the online world entirely.[7] The consequences of these attacks can be felt in the real world, impacting targets' personal lives and putting them in fear for their safety.[8] The most common targets are women who are singled out and attacked online with violent threats of physical and sexual assault.[9] Racist, homophobic, and anti-religious attacks are also prevalent.[10] According to Danielle Citron, a key element in the rise of these attacks is that the speakers remain anonymous: "Individuals say and do things online that they would never consider saying or doing offline because they feel anonymous . . . ."[11] Whereas anonymity has been traditionally viewed as a shield for the individual against tyranny, in this context it enables a majority to terrorize the few.

The rise of online harassment challenges the traditional justifications for anonymous speech. The most common argument for anonymity is that it increases the ability of people to speak, and protects speech that might not otherwise be heard. Harassment under cover of anonymity, however, can stifle

6. *See, e.g.*, Mattathias Schwartz, *Inside the World of Online Trolls, Who Use the Internet To Harass, Humiliate and Torment Strangers: Mal*web*olence*, N.Y. TIMES, Aug. 3, 2008 (Magazine), at 24.

7. *See, e.g.*, *Blog Death Threats Spark Debate*, BBC NEWS, Mar. 27, 2007, http://news.bbc.co.uk/1/hi/technology/6499095.stm (describing the concerted verbal attacks on Kathy Sierra, a well-known technology blogger, that prompted her to cancel her public appearances and shut down her blog).

8. *See, e.g.*, Peter Lattman, *Boalt Student Posts "Copycat Threat" to Hastings*, Law Blog—WSJ.com, Apr. 20, 2007, http://blogs.wsj.com/law/2007/04/20/boalt-student-allegedly-posts-copycat-threat-to-hastings-law; Mitch Wagner, *Death Threats Force Designer To Cancel ETech Conference Appearance*, InformationWeek, Digital Life Weblog, Mar. 26, 2007, http://www.informationweek.com/blog/main/archives /2007/03/death_threats_f.html.

9. The volunteer organization Working To Halt Online Abuse reports that more than seventy percent of the victims of online harassment it has worked with since 2000 have been women. Working To Halt Online Abuse, Comparison Statistics 2000-2007, http://www.haltabuse.org/resources/stats/Cumulative2000-2007.pdf (last visited Oct. 27, 2008).

10. *See, e.g.*, Schwartz, *supra* note 6; Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. (forthcoming 2009) (manuscript at 17-18, on file with author).

11. Citron, *supra* note 10, at 21.

the speech of its targets. Indeed, those overwhelmingly targeted by online harassment—members of social minorities—are those most in need of protection. Silencing the contributions of the targets of online harassment "impoverish[es] the dialogue society depends upon for purposes great and small."[12] Thus, anonymous harassing speech may reduce, rather than enhance, the amount and quality of online speech.

Legal enforcement in this vast and changing environment is precariously balanced on a single procedural tool: the John Doe subpoena. Because of the unique structure of the Internet, the identities of most supposedly "anonymous" posters, while impenetrable to the casual observer, are tracked and stored by the websites on which they post and by the Internet service providers (ISPs) that provide them with Internet access.[13] John Doe subpoenas allow plaintiffs to discover the identity of anonymous online speakers from their ISP or from websites they visited. Without a successful John Doe subpoena, a target of anonymous online speech has no way to uncover his or her attackers and no legal remedy. Although John Doe subpoenas are procedural tools, the standards governing them define the extent of First Amendment rights online. A standard that is too permissive severely weakens the ability of citizens to speak anonymously, limiting freedom of speech online. Too restrictive a standard leaves the increasing litany of targets of online harassment with no defense. Only a consistent nationwide standard for John Doe subpoenas will ensure balanced protection for both anonymous online speakers and the targets of anonymous online speech.

Despite their importance, John Doe subpoenas have no such single standard. No fewer than seven different cases[14] have expressed distinct standards over the past nine years. These standards vary widely, making the extent of the right to anonymous speech online uncertain. Although recent standards have begun to achieve a measure of consistency, they are just beginning to be tested against the rise of online harassment. This Note will examine John Doe subpoenas, their history, and the standards that govern them. Based on this analysis, it will evaluate the emerging consensus of recent standards and recommend a single, consistent standard that fairly balances the interests of plaintiffs and defendants and is flexible enough to address the emerging paradigms of anonymous online speech.

12. *Id.* at 24.

13. *See, e.g.*, Richard Morgan, *A Crash Course in Online Gossip*, N.Y. TIMES, Mar. 16, 2008, at ST7.

14. *See infra* note 61.

Part I of this Note examines the history of John Doe pleadings, the procedure of modern John Doe subpoenas, and the unique challenges they present. Part II argues that John Doe subpoena standards should be structured to afford less anonymity to online speakers who chill more speech than they create. Part III breaks John Doe subpoena standards down into six constituent factors and evaluates what level of each factor is appropriate to balance the interests of both plaintiffs and defendants. Part IV closes by presenting a single standard that will fairly balance the First Amendment interests of both plaintiffs and defendants, and by applying this proposed standard to a recent online controversy.

I. WHAT IS A JOHN DOE SUBPOENA?

A. The Qualified Privilege of Anonymous Speech

In *McIntyre v. Ohio Elections Commission*, the Court concluded that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[15] The Court based *McIntyre* on two grounds—one of public concern and one of private concern. First, "'[a]nonymity is a shield from the tyranny of the majority' without which public discourse would certainly suffer."[16] Second, the author's decision to identify himself should be a question of authorial autonomy: "[A]n author generally is free to decide whether or not to disclose his or her true identity."[17] Since then, the Court has extended this logic to "the vast democratic forums of the Internet,"[18] which "would be stifled if users were unable to preserve their anonymity online."[19]

15. 514 U.S. 334, 342 (1995); *see also id.* at 345 (ruling that an Ohio law that forbade any publication promoting a ballot issue unless it contained the "name and residence" of the author was unconstitutional).

16. Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1543 (2007) (quoting *McIntyre*, 514 U.S. at 357).

17. *McIntyre*, 514 U.S. at 341.

18. Reno v. ACLU, 521 U.S. 844, 868 (1997).

19. David L. Sobel, *The Process That "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3, ¶ 5 (2000), http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html; *see also McIntyre*, 514 U.S. at 357 ("Anonymity is a shield from the tyranny of the majority."). *But see* Caroline E. Strickland, Note, *Applying* McIntyre v. Ohio Elections Commission *to Anonymous Speech on the Internet and the Discovery of John Doe's Identity*, 58 WASH. & LEE L. REV. 1537, 1580-82 (2001) (arguing that *Mcintyre* has been wrongly applied

Whether online or offline the right to anonymous speech is not absolute. Lyrissa Lidsky recently argued that the "right" to anonymous speech is better termed a "[q]ualified [p]rivilege,"[20] as it is "not absolute but must be balanced against plaintiffs' interests."[21] According to Lidsky, "[s]peakers may use the shield of anonymity for a variety of purposes, only some of which may be consistent with the public good."[22] Understanding the extent of this qualified privilege requires a better understanding of the process of John Doe subpoenas.

B. From John Doe Pleading to John Doe Subpoenas

Suits involving fictitious parties are a longstanding legal phenomenon.[23] John Doe was first conceived as "an entirely fictional character," on whose behalf plaintiffs could bring suits.[24] Later, this technique was used to enable the initiation of proceedings against as yet unknown defendants. Civil rights cases against law enforcement were the most common example of this technique, where plaintiffs sued a set of unnamed police officers.[25] Without a pseudonymous John Doe, the plaintiff cannot file his suit until he knows the identity of his defendant(s), and thus cannot rely on court-sanctioned discovery tools to identify them. Allowing plaintiffs to sue Doe defendants permits them to "start discovery while candidly acknowledging that [they do] not yet know the correct identity of the defendant."[26]

The rise of the Internet has brought an explosion of John Doe lawsuits. While the identities of online speakers are impenetrable to most users, companies running online message boards or connecting posters to the Internet can often discover them. If someone discovers that a person is posting

to anonymous speech online because, among other things, it was focused on prior restraint of speech).

20. Lidsky & Cotter, *supra* note 16, at 1599.

21. *Id.* at 1600.

22. *Id.* at 1559.

23. *See generally* Carol M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure To Recognize John Doe Parties*, 57 U. PITT. L. REV. 883, 889 (1996) (tracing the history of John Doe pleadings).

24. *Id.* at 890 & n.22.

25. *See, e.g.*, Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (holding that a cause of action existed for a plaintiff who was searched and arrested without a warrant); Screws v. United States, 325 U.S. 91 (1945) (holding local law enforcement officers accountable for beating a suspect to death).

26. Rice, *supra* note 23, at 897.

violent and sexual threats about them on a message board, for instance, one of the earliest steps in any legal response that they mount will be to seek the poster's identity. Uncovering this identity often requires two steps. First, the plaintiff must subpoena the website, or online service provider (OSP), for the Internet protocol (IP) address of the user who made the online comments. Assuming that the website has the information—many websites store the IP addresses of the users who visit them, but some do not—it can provide the plaintiff with the IP address of the poster. The IP address is a string of numbers that identifies the computer, though not the person, that posted the comment to the website.[27]

IP addresses, however, do not remain tied to an individual computer. Each ISP owns a pool of IP addresses that it provides to its customers, often issuing each customer a new IP address each time he connects to the Internet. Only the ISP knows what IP address was attached to which computer at any given time. Thus, the plaintiff must file another subpoena targeting the poster's ISP, seeking the address, telephone number, and other contact information associated with the account of the computer whose IP address he received from the OSP. Often, the ISP will be able to identify both the computer using the targeted IP address and the account information of that computer's owner. This only establishes that the account owner was responsible for the computer that was used to publish the speech in question. Unless the computer is stored in a public space, or the account owner argues that some specific third party used the computer without his permission, this is often enough for the plaintiff to amend his complaint with the account owner's name as his defendant and proceed with his suit. Assuming that the defendant has been properly notified, he may anonymously move to quash one or both of the subpoenas. Because defendants are much more likely to be notified by their ISP than by an OSP, the initial IP address subpoena is rarely challenged in court.[28]

Because John Doe subpoenas are the central tool for litigation in this area, the standard that governs them effectively determines the breadth of the right to anonymous speech on the Internet. A standard that is too weak decimates the protection of anonymity, allowing plaintiffs to "pursue . . . extra-judicial self-help remedies"[29] by unmasking defendants who have said nothing

27. For a more detailed discussion of IP addresses and Internet infrastructure, see Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV 653, 656-69 (2003).

28. *See infra* Subsection III.B.1.

29. Doe No. 1 v. Cahill, 884 A.2d 451, 457 (Del. 2005). For a classic example of plaintiff "self-help," see Kaitlin Quistgaard, *Raytheon Triumphs over Yahoo Posters' Anonymity*, SALON.COM, May 24, 1999, http://www.salon.com/tech/log/1999/05/24/raytheon/index.html.

actionable and "simply seek revenge or retribution."[30] On the other hand, "anonymity may . . . serve as a shield to hide behind, leaving a defamed plaintiff without a potential defendant."[31] In determining whether to protect a defendant, courts must distinguish between instances in which anonymity is critical, such as "governmental whistleblowing; labor organizing; dissident movements in repressive countries; gay and lesbian issues; and resources dealing with addiction, alcoholism, diseases and spousal abuse,"[32] and contexts in which it is not, such as defamation and harassment. John Doe subpoenas must somehow thread this procedural needle, enabling courts to determine when anonymity is an unscrupulous cloak and when it is a deserved shield.

C. The Unique Features of John Doe Subpoenas

The challenges facing John Doe subpoenas stem from three related factors: severity, timing, and notice. These three characteristics make balancing the interests at stake particularly delicate. Because of these concerns, traditional pleading rules may be insufficient to the task. First, John Doe subpoenas can have severe consequences, potentially causing irreparable harm to defendants if granted, and denying plaintiffs the opportunity to seek relief for their harms if denied. A defendant who is exposed could be subject to reprisals[33] or severe social and professional sanctions, making extreme care necessary when exposing potentially innocent defendants. At the same time, a plaintiff who is denied the identity of his defendant is left with no recourse and has his suit effectively denied without a hearing on the merits.

Second, John Doe subpoenas occur very early in the process of the trial, as an element of expedited discovery that usually happens shortly after the filing of the lawsuit. This exacerbates the problem of severe consequences by pairing them with insufficient consideration. Further, a John Doe subpoena is rarely served in the same court as the original case was brought—in the age of the Internet, the headquarters of ISPs and OSPs are scattered across jurisdictions. Thus, the court making this ruling will likely be different than the court where the subpoena was filed and will not have the benefit of previous experience or a ruling on the merits to guide its decision.

---

30. *Cahill*, 884 A.2d at 457.

31. Scot Wilson, Comment, *Corporate Criticism on the Internet: The Fine Line Between Anonymous Speech and Cybersmear*, 29 PEPP. L. REV. 533, 537 (2002).

32. Sobel, *supra* note 19, ¶ 6.

33. *See, e.g.*, Quistgaard, *supra* note 29.

Finally, although a motion to quash may well be appropriate, without proper notice, John Doe subpoenas can easily become ex parte proceedings. In many jurisdictions, defendants must rely on the business policies of the subpoena's target or the goodwill of the plaintiff to receive notice. Even if the plaintiff does attempt to notify the defendant, he could fail—the defendant is, after all, anonymous. If the subpoena becomes ex parte, one of the defendant's most important defenses—his own vigorous advocacy—is eliminated. This combination of severe consequences meted out after limited trial process, possibly without opposition from the defendant whose identity is at risk, is a dangerous recipe that demands a carefully balanced standard.[34]

II. DISTINGUISHING ONLINE HARASSMENT FROM TRADITIONAL ANONYMOUS ONLINE SPEECH

The rise of online harassment, and especially public harassment of individuals by anonymous groups, further complicates the traditional analysis of anonymous speech. The right to anonymous speech is often defended because it increases participation in public debate.[35] Anonymous online harassment, however, can frighten its targets into silence and drive them out of public debate entirely. Because it largely targets minority groups, online harassment has repercussions beyond its immediate targets, potentially dissuading entire classes of speakers from public speech. Danielle Citron likens modern online mobs to the "anti-immigrant mobs of the nineteenth century and the Ku Klux Klan."[36] In this context, the identification of a speaker can be a powerful tool to combat the chilling effect of online harassment. Indeed, according to Citron, anonymity is one of the key features of the online environment that encourages such harassment: "Because group members often shroud themselves in pseudonyms, they have little fear that victims will

34. Michael Vogel has argued that John Doe subpoenas rely on "relatively mundane rules of civil procedure" and that courts "should be hesitant to imply new procedural rules without clear proof that existing rules are inadequate." Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing over Legal Standards*, 83 OR. L. REV. 795, 840-41 (2004). This Note does not respond to Vogel point by point, but it asserts at least three specific reasons why existing pleading rules are, in fact, inadequate: severe consequences, occurrence of John Doe subpoenas early in trial, and possible lack of opposition from an uninformed defendant.

35. For an in-depth analysis of the costs and benefits of anonymous speech, see Lidsky & Cotter, *supra* note 16, at 1578-79.

36. Citron, *supra* note 10, at 19.

retaliate against them . . . ."[37] Exposing the identity of online speakers eliminates this feeling of immunity and replaces it with one of accountability.

Regardless of the rising incidence of online harassment, anonymity is still a vital shield to protect valuable speech—particularly criticism of powerful public figures. Stripping anonymity away in these cases would make people less willing to speak, limiting the Internet's potential to generate widespread public debate. If John Doe subpoenas are to appropriately protect speech online, they must balance the concerns of traditional anonymous speech with those raised by anonymous online harassment.

John Doe subpoenas arise as part of many legal claims, including defamation, trademark infringement, and even trespass to chattels.[38] For a standard to balance fairly the interests of plaintiffs and defendants, it must evaluate whether the substance of the plaintiff's claim is strong enough to merit unmasking the defendant. Although John Doe subpoenas arise under varied substantive claims, they all affect the right to anonymous speech online. To accomplish this task, the standard should distinguish between anonymous speech that enhances public discourse and anonymous speech that chills it. All anonymous speech should be procedurally protected, but the bar that a plaintiff must meet to expose a speaker of nonchilling anonymous speech should be higher.

Courts have been most willing to protect speech that contributes to important public debate.[39] Although such speech may be harsh, vulgar, or rude, protecting language that may be distasteful is necessary to ensure that the debate itself may continue. At the same time, "[n]either the intentional lie nor the careless error materially advances society's interest in" public debate.[40] In identifying speech that especially merits due protection in a defamation context, the Court's inquiries have centered on whether the target of the speech was a public figure. Regardless of the legal claim under which they arise, John Doe subpoenas regulate the breadth of protected speech just as defamation law does. Thus, public figure doctrine, adapted to the context of anonymous online

37. *Id.* at 21.

38. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999) (considering identification of an anonymous defendant in a trademark infringement claim); Mobilisa, Inc. v. Doe 1, 170 P.3d 712 (Ariz. Ct. App. 2007) (considering a John Doe subpoena in a claim of trespass to chattels); Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005) (considering a John Doe subpoena in a defamation claim).

39. *See, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964) ("[D]ebate on public issues should be uninhibited, robust, and wide-open . . . .").

40. Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974).

speech, can be a useful method to separate online harassment from public debate.

A. Public Figure Doctrine

Public figure doctrine focuses on the status of the actor rather than the content of the speech. In *New York Times Co. v. Sullivan*, the Court concluded that public officials had to meet an increased standard of liability to prove defamation.[41] *Curtis Publishing Co. v. Butts* expanded upon this even further when it concluded that "criticism of private citizens who seek to lead in the determination of . . . policy [cannot] be less important to the public interest than . . . criticism of government officials."[42] This description could include celebrities, political leaders, and corporations.

Gertz identified two distinctive features of public figures. First, they "achieve that status voluntarily," opening them "to greater media scrutiny and thus weaken[ing] their claim to protection from reputational harm."[43] Second, their increased access to traditional media such as television and newspapers "enables them to redress the harms inflicted by defamatory publications through corrective speech."[44] Thus, *Gertz* identified public figures as (1) having voluntarily acceded to publicity, and (2) being especially well equipped to respond to actionable speech.

The Court has also identified two narrower types of public figures: limited-purpose public figures and involuntary public figures. While public figures must demonstrate actual malice for any defamation suit that they bring, limited-purpose public figures must do so only regarding the particular controversy in which they are embroiled.[45] Limited-purpose public figures must "have thrust themselves to the forefront of particular public controversies

41. 376 U.S. at 279-80 ("The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' . . . .").

42. 388 U.S. 130, 148 (1967) (quoting Pauling v. Globe-Democrat Publ'g Co., 362 F.2d 188, 196 (8th Cir. 1966)).

43. Aaron Perzanowski, *Relative Access to Corrective Speech: A New Test for Requiring Actual Malice*, 94 CAL. L. REV. 833, 841 (2006).

44. *Id.* at 842.

45. *Gertz*, 418 U.S. at 352 (finding that, because plaintiff was not a public figure in the controversy concerning which he was defamed, the actual malice standard did not apply).

in order to influence the resolution of the issues involved."[46] *Time, Inc. v. Firestone* held that "public controversy" did not simply mean topics that sparked the public interest.[47] In that case, mere prurient fascination with the breakup of a socialite's marriage was of public interest, but not a public controversy.[48] Other than suggesting that a public controversy must be significant, however, the Court has done little to define the concept.[49] While it is certainly narrower than the full scope of issues that may be of interest to the public, its boundaries remain uncertain. What plaintiffs must have done to "thrust themselves to the forefront" of a controversy is similarly defined mostly by exclusion.[50] *Firestone*, for instance, concluded that "a few press conferences" focused on the plaintiff's experiences were insufficient to make the plaintiff a public figure.[51] As this suggests, the exact delineation of the class of limited-purpose public figures remains murky.

Closely related to the limited-purpose public figure is the involuntary public figure. According to *Gertz*, "it may be possible for someone to become a public figure through no purposeful action of his own, but the instances of truly involuntary public figures must be exceedingly rare."[52] In other words, an individual who simply finds himself at the center of important societal events

46. *Id.* at 345. Lower courts have sought to add detail to this definition. The Fourth Circuit, for instance, identified the five requirements for a limited-purpose public figure as: (1) the plaintiff had access to channels of effective communication, (2) the plaintiff voluntarily assumed a role of special prominence in a public controversy, (3) the plaintiff sought to influence the resolution or outcome of the controversy, (4) the controversy existed prior to the publication of the defamatory statements, and (5) the plaintiff retained public figure status at the time of the alleged defamation. Fitzgerald v. Penthouse Int'l, 691 F.2d 666, 668 (4th Cir. 1982); *see* Reuber v. Food Chem. News, Inc., 925 F.2d 703, 708 (4th Cir. 1991).

47. 424 U.S. 448, 454 (1976).

48. *See id.*

49. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 539-40 (2001) (Breyer, J., concurring) (arguing that a dispute between a teacher's union and a school board was a public controversy); Lorain Journal Co. v. Milkovich, 474 U.S. 953, 964 n.9 (1985) (Brennan, J., dissenting) (claiming that a debate over a fistfight at a high school wrestling match was a public controversy in part because it "was not a private matter of public concern merely to gossips").

50. *See, e.g.*, Hutchinson v. Proxmire, 443 U.S. 111, 135 (1979) (holding that a scientist who was awarded a mock award for wasteful government spending was not a public figure because he was not a significant figure in any public controversy); Wolston v. Reader's Digest Ass'n, 443 U.S. 157, 166 (1979) (holding that the petitioner, who was being investigated in an espionage case and had refused to appear before a grand jury, was not at the forefront of a public controversy).

51. 424 U.S. at 454-55 n.3.

52. Gertz v. Robert Welch, Inc., 418 U.S. 323, 345 (1974).

could, in certain circumstances, be thrust into the role of a public figure. Like limited-purpose public figures, involuntary public figures have been mentioned in only a handful of Supreme Court cases beyond *Gertz*. *Firestone* approvingly cited an academic article "concluding that the *Gertz* opinion suggests a 'category of involuntary public figures' roughly equivalent to 'individual[s] involved in or affected by . . . official action.'"[53] The Court in *Hutchinson v. Proxmire* stated that "those charged with defamation cannot, by their own conduct, create their own defense by making the claimant a public figure,"[54] suggesting that a plaintiff cannot be transformed into an involuntary public figure by the very action that prompted his lawsuit. Most lower courts have been as reticent to find an involuntary public figure as the Court has been in discussing the concept.[55]

Public figure doctrine remains vague in part because it is designed to manage a wide range of varying contexts. It was developed to maintain a balance between the interests of private individuals and the need for vigorous debate on public issues. John Doe subpoenas manage this same balancing act. With some adaptation, public figure doctrine can be used to distinguish between anonymous online harassment and anonymous public debate, making it possible to distinguish which online speakers' anonymity is due particularly high protection.

B. Adapting the Public Figure Standard to Anonymous Online Speech

In the three decades since the public figure doctrine was first introduced, the Internet has upended the "centralized, concentrated, and powerful one-to-many media"[56] that was the basis of the original doctrine. Courts face two particular shifts when applying the legal concept of the public figure to the online environment: (1) public figures' advantage over private figures in responding to attacks is reduced online, and (2) the likelihood that an individual would be thrust into public view is greatly increased. If courts do

53. *Firestone*, 424 U.S. at 476 n.4 (quoting David A. Anderson, *Libel and Press Self-Censorship*, 53 TEX. L. REV. 422, 450-51 (1975)).

54. 443 U.S. 111, 135 (1979).

55. *See, e.g.*, Lohrenz v. Donnelly, 350 F.3d 1272, 1278 (D.C. Cir. 2003) (finding that the defendant was a limited-purpose public figure, not an involuntary public figure); Wells v. Liddy, 186 F.3d 505, 540 (4th Cir. 1999) (finding that the defendant was not an involuntary public figure). *But see* Dameron v. Washington Magazine, Inc., 779 F.2d 736 (D.C. Cir. 1985) (identifying an air traffic controller on duty at the time of a crash as an involuntary public figure).

56. Perzanowski, *supra* note 43, at 850.

not maintain a narrow definition of public figures online, these characteristics could result in a wide expanse of online public figures without the remedial advantages or voluntariness that play such important roles in justifying their reduced legal protection.

First, because anyone can easily publish speech on the Internet, the effect of public figures' "significantly greater access to the channels of effective communication" is limited.[57] Because of this, the advantage that public figures enjoy over private figures in responding to online speech is limited. Further, a target of anonymous speech will likely have no information about his assailant's motivation, experience, or knowledge, and will be subjected to enhanced public scrutiny, while his assailant will remain protected. This makes anonymous speech particularly hard to rebut, limiting the impact of the little increased access that public figures retain. These factors combine to significantly reduce the advantage public figures enjoy online.

Second, the range of issues that can capture global attention and push a person into the limelight is much broader in the age of the Internet. A single video, posted to YouTube, is all that is required to start a phenomenon.[58] Because online speech is inexpensive, long-lasting, and far-reaching, it is difficult to predict what speech will seize enough public attention to transform its speaker into a public figure. This undermines the notion of voluntary accession to publicity that is inherent in the public figure doctrine.

Third, the uncertainty of whether online speech will transform its speaker into a public figure may dissuade people from contributing to the public sphere. Faced with reduced legal protection, potential speakers may avoid speaking if they risk transforming themselves into public figures. While true public figures have to accept this bargain in order to ensure robust public debate, the lower the threshold, the more those not seeking publicity will refrain from even limited contribution, and the less participatory the public sphere will become. For all three of these reasons, courts should be particularly cautious when designating a plaintiff an online public figure, lest they premise their ruling on characteristics that do not apply in the online context and so dissuade public engagement.

One final complication is how to classify a target of anonymous speech who chooses to respond with more speech. Because responding to harmful speech with more speech increases public debate, while responding with litigation can

57. Gertz v. Robert Welch, Inc., 418 U.S. 323, 344 (1974); *see also* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("[A]ny person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox.").

58. *See, e.g.*, Tu Thanh Ha, *supra* note 5.

limit it, the targets of such speech should be encouraged to respond with more speech whenever possible.[59] In an online world, where even private figures often have some access to media, responding to an attack with more speech could transform a private citizen into a limited-purpose public figure. If this were the case, however, targets would face perverse incentives to either remain silent or immediately respond to any potentially actionable statement with a lawsuit. Both of these outcomes reduce engagement in the public sphere, and the latter would lead to an increase in costly litigation. *Firestone* concluded that a plaintiff who gave several interviews regarding her ongoing lawsuit was not a limited-purpose public figure, because her case—the subject of the interviews—did not constitute a public controversy, and her efforts could not affect its outcome.[60]

To give plaintiffs incentives to attempt corrective speech before resorting to litigation, courts should be similarly cautious about designating limited-purpose public figures online. Plaintiffs should not be considered limited-purpose public figures except when they clearly attempt to move beyond their personal situation and influence a larger debate, such as when a woman who is attacked online launches a campaign to raise awareness about online harassment of women. Courts should be cautious even here, however, as any target who responds with speech will have to reference broader solutions and questions to some degree. A plaintiff should have repeatedly thrust herself to the forefront of a debate, reaching beyond her personal experience, before she is designated a limited-purpose public figure.

C. Distinguishing Between Chilling and Nonchilling Speech

The public figure standard, as adapted to an online context, can be used to identify when public anonymous speech deserves greater or lesser protection. Public speech directed at a public figure should receive the highest protection, while nonpublic speech or speech directed at a private figure should receive less. Courts should be especially cautious when designating a speaker a public figure. A target of anonymous speech should not be designated a limited-purpose or involuntary public figure unless (1) his status is derived from events that took place before the speech that is at issue; or (2) he holds himself forth as an advocate beyond simply responding to the speech in question.

---

59. *See, e.g.*, Curtis Publ'g Co. v. Butts, 388 U.S. 130, 153 (1967) ("[S]peech can rebut speech, propaganda will answer propaganda, free debate of ideas will result in the wisest government policies." (quoting Dennis v. United States, 341 U.S. 494, 503 (1951)) (internal quotation marks omitted)).

60. Time, Inc. v. Firestone, 424 U.S. 448, 454-55 (1976).

Having identified a test to distinguish between types of anonymous speech, the next Part of this Note develops a single, consistent standard to evaluate John Doe subpoenas. In so doing, it imports the public figure standard discussed here into the broader test, proposing a final standard that fairly balances the interests of plaintiffs and defendants.

III. EVALUATING THE CURRENT STANDARDS AND DEVELOPING A SINGLE BALANCED STANDARD

Over the past decade, courts have adopted at least seven standards for evaluating John Doe subpoenas.[61] These standards rely on a wide range of factors with requirements that vary from permissive to stringent. As a result, the standards themselves range from pro-plaintiff[62] to pro-defendant.[63]

Rather than comparing existing John Doe subpoena standards as indivisible packages, this Note identifies six major factors that the standards share. By analyzing these individual factors, rather than the standards as a whole, it develops a hybrid standard that combines the strengths of the different standards into a single, balanced proposal. The six factors of John Doe subpoenas are: (1) ensuring the defendant has notice and opportunity to respond to the subpoena before his identity is exposed, (2) evaluating the strength of the plaintiff's case, (3) determining the relevance of the information sought by subpoena to the plaintiff's claim, (4) balancing the interests of the plaintiff and defendant, (5) requiring that the plaintiff make his claim and demonstrate his evidence with specificity, and (6) requiring that the plaintiff exhaust all alternatives for identifying the plaintiff before turning to a John Doe subpoena.

Each of these factors will be examined in detail. Before turning to a close factor-by-factor analysis, however, it is useful to consider the standards that courts have proposed thus far. This Part begins by briefly introducing the major John Doe subpoena cases in chronological order. It notes other legal contexts in which similar challenges arise and identifies the themes that have

61. *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); Mobilisa, Inc. v. Doe 1, 170 P.3d 712 (Ariz. Ct. App. 2007); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Ct. App. 2008); Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005); Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *In re* Subpoena Duces Tecum to Am. Online, Inc. (*In re AOL*), 52 Va. Cir. 26 (Cir. Ct. 2000), *rev'd on other grounds sub nom*. Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

62. *See In re AOL*, 52 Va. Cir. 26.

63. *See Dendrite*, 775 A.2d 756.

marked the development of John Doe subpoena standards in recent years. Then it considers the six major factors of John Doe subpoena standards one-by-one. It determines which factors are necessary for a comprehensive standard and sets a bar for each factor that balances the needs of plaintiffs and defendants. As it proceeds, Part III incorporates the First Amendment analysis discussed in Part II to determine whether the defendant's identity should be discoverable.

A. Existing John Doe Subpoena Standards

When considering an emerging area of law such as John Doe subpoenas, analysis often begins with other areas of law that manage similar concerns. There are at least three areas of law where courts have considered similar challenges. First, courts evaluating reporters' claims of privilege to protect anonymous sources must weigh questions of disclosure and speech.[64] Second, courts considering strategic lawsuits against public participation (SLAPPs) must balance the interests of a defendant claiming that a lawsuit was brought only to silence and intimidate him against the interests of a plaintiff claiming to be seeking deserved redress for harm.[65] Third, the Digital Millennium Copyright Act (DMCA) provides a statutory framework for third-party subpoenas seeking the identity of copyright infringers.[66] While academic authors have argued that these areas of law provide useful templates for developing general-purpose John Doe subpoena standards,[67] courts have

64. *See, e.g.*, Zerilli v. Smith, 656 F.2d 705 (D.C. Cir. 1981) (upholding the journalist's privilege, even though the information sought was crucial to the plaintiff's case, because alternative methods to access the information had not been exhausted); Dangerfield v. Star Editorial, Inc., 817 F. Supp. 833 (C.D. Cal. 1993) (holding that the First Amendment privilege against disclosure could be overcome by a showing of compelling need); Mitchell v. Superior Court, 690 P.2d 625 (Cal. 1984) (articulating a standard to evaluate discovery of a reporter's anonymous source, and ruling that it was not merited in that case).

65. *See, e.g.*, Global Telemedia Int'l Inc. v. Doe, 132 F. Supp. 2d 1261 (C.D. Cal. 2001) (dismissing a cyber-SLAPP suit brought under CAL. CIV. PROC. CODE § 425.16 (West 2004), California's anti-SLAPP statute, by employing a balancing test).

66. 17 U.S.C. § 512(h) (2000); *see* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003) (applying the DMCA standard); Trevor A. Dutcher, Comment, *A Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in* RIAA v. Verizon Internet Services, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 493 (2005) (discussing the mechanics of DMCA John Doe subpoenas). At least one court has evaluated a John Doe subpoena for a copyright infringer outside of the DMCA context. *See* Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

67. *See, e.g.*, Shaun B. Spencer, *CyberSLAPP Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493 (2001); Sean P.

preferred instead to base their standards on fundamental First Amendment principles. In so doing, courts have adopted many of the key factors of privilege and anti-SLAPP into their standards, making it possible to analyze them directly in the context of John Doe subpoenas.[68] Thus, although this Note will indicate where parallel legal standards are relevant, it focuses on the seven standards courts have developed to deal directly with John Doe subpoenas, which this Section now turns to consider.

The seven major John Doe subpoena standards can be divided into two rough groups. The first four standards, adopted between 1999 and 2001, are examples of early forays and experimentation by courts in addressing this new field. The three most recent standards, established between 2005 and 2008, represent the beginning of a growing consensus among courts.

In the first case to consider the difficulties of identifying a defendant online, *Columbia Insurance Co. v. Seescandy.com*,[69] the plaintiff alleged that two of the defendant's websites infringed upon his trademark. The court refused to grant an injunction unless the defendant could be located, and established a fairly weak standard to govern the release of an anonymous defendant's identity. The plaintiff had to (1) demonstrate that his claim was strong enough to survive a motion to dismiss,[70] (2) demonstrate that the information that he sought would likely lead to identifying the defendant and thus was relevant to his claim,[71] and (3) identify all previous steps he had taken to locate the defendant.[72]

Not long after *Seescandy.com*, an anonymous company sued five posters who had allegedly defamed it in an America Online (AOL) chat room. AOL sought to quash the subpoena in Virginia state court. The standard that the court expressed in *In re Subpoena Duces Tecum to America Online, Inc.* (*In re*

Trende, *Defamation, Anti-SLAPP Legislation, and the Blogosphere: New Solutions for an Old Problem*, 44 DUQ. L. REV. 607 (2006); Joseph R. Furman, Comment, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation*, 25 SEATTLE U. L. REV. 213 (2001); Megan M. Sunkel, Comment, *And the I(SP)s Have It . . . But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking To Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C. L. REV 1189, 1189 (2003).

68. At least one author has advocated applying the standard from *Dendrite*, 775 A.2d 756, to the context of the DMCA. *See* Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222 (2004). *Sony Music Entertainment Inc.* also incorporated factors from several of the cases closely analyzed in this Note. 326 F. Supp. 2d at 564-65.

69. 185 F.R.D. 573 (N.D. Cal. 1999).

70. *Id.* at 579.

71. *Id.* at 580.

72. *Id.* at 579.

AOL)[73] included three factors (overlapping, but not identical to *Seescandy.com*): (1) the strength of the plaintiff's argument, (2) the relevance of the information sought, and (3) the specificity of the plaintiff's evidence.[74] Although the *Seescandy.com* decision had not posed strong protection for the anonymity of its defendant, the *AOL* standard was in fact weaker in at least one key respect: the plaintiff needed only a "good faith basis" for his claim—a significantly lower requirement than *Seescandy.com*'s motion to dismiss standard.[75]

Dendrite International, Inc. v. Doe, No. 3 also concerned a company suing anonymous bulletin board posters for allegedly defamatory statements.[76] *Dendrite* was the first standard to provide robust protection for anonymous defendants. It required that the plaintiff demonstrate a prima facie case—a higher bar than either *In re AOL* or *Seescandy.com*.[77] *Dendrite* also included two new factors. First, it required that the plaintiff attempt to notify the defendant, and afford him a reasonable opportunity to respond—key steps if a defendant is to be able to protect his anonymity. Second, *Dendrite* introduced a balancing factor, directing the court to "balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure."[78] This provided flexibility to judges faced with a landscape of rapidly evolving technology and law, and gave them an avenue to consider concerns that were outside the scope of earlier standards, such as the potential for the defendant to be harmed if his identity were revealed. *Dendrite* was a significant early development in John Doe subpoena standards, and it has been extensively cited by courts developing subsequent standards.

The final early John Doe subpoena decision, *Doe v. 2TheMart.com Inc.*,[79] was another first—the first time that a plaintiff used a John Doe subpoena to seek the identity of not only defendants, but also nonparty witnesses. In *2TheMart.com*, the plaintiff corporation subpoenaed the identity of twenty-

73. 52 Va. Cir. 26 (Cir. Ct. 2000).

74. *Id.* at 37.

75. *Id.*

76. 775 A.2d 756, 763 (N.J. Super. Ct. App. Div. 2001). *Dendrite* affirmed the denial of the plaintiff's motion to discover the defendant's identity. *Id.* at 772. On the same day, the same court applied an identical standard in *Immunomedics, Inc. v. Doe*, 775 A.2d 773, 777 (N.J. Super. Ct. App. Div. 2001), but came to the opposite conclusion.

77. *Id.* at 760. *Seescandy.com* required that the plaintiff "identify all previous steps taken to locate the elusive defendant," 185 F.R.D. at 579 (N.D. Cal. 1999), but did not specify what level of notice was actually required.

78. 775 A.2d at 760.

79. 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

three posters that had taken part in a vitriolic discussion about it on an anonymous online message board. Despite the fact that the plaintiff had broadened its search to the identities of nonparties, the standard that the court settled on was no stronger than *In re AOL*'s, requiring only that the plaintiff show a good-faith belief in his claim and that the information that he sought was both relevant and unavailable from any other source.[80] Although the court expressed a weak standard, it nevertheless refused discovery of the identities, finding that 2TheMart.com had "failed to demonstrate that the identity of the Internet users [was] directly and materially relevant to a core defense."[81]

These first four major John Doe subpoena cases, all of which occurred between 1999 and 2001, have several common characteristics. First, only one of them—*Dendrite*—contained a notice provision or balancing test.[82] Second, again with the exception of *Dendrite*, they provided relatively low bars, making it likely that plaintiffs could unmask anonymous defendants. Third, although all of the standards considered the strength of the plaintiff's argument and the relevance of the information that he sought, the other factors that they incorporated varied widely. Thus, these early standards describe a pattern of experimentation by courts centering around fairly weak protection for the anonymity of online speakers. More recent John Doe subpoena cases have begun to change this pattern.

Doe No. 1 v. Cahill,[83] decided in 2005, marked the beginning of a rise in individuals—as opposed to companies—seeking John Doe subpoenas. Mr. Patrick Cahill, a city councilman, sought the identity of a poster who had attacked him on a blog.[84] He received the defendant's IP address from the online message board without opposition,[85] and then sued the Doe's ISP to discover his identity.[86] The ISP notified the defendant, who filed an emergency motion.[87] *Cahill* adopted what the court termed "a modified *Dendrite* standard" that included only two of *Dendrite*'s five elements.[88] It retained *Dendrite*'s

80. *See id.* at 1095.

81. *Id.* at 1096.

82. 775 A.2d at 760.

83. 884 A.2d 451 (Del. 2005).

84. *Id.* at 454.

85. The court provides no indication that the defendant received notice of the release of his IP address. *Id.*

86. *Id.* at 454-55.

87. *Id.* at 455.

88. *Id.* at 461.

notice requirement,[89] and included a modified strength-of-argument factor that required the plaintiff to demonstrate a claim strong enough to survive an adverse motion for summary judgment—which, within the *Cahill* court's jurisdiction, required the same prima facie evidentiary showing as *Dendrite* had called for.[90] Because Cahill was a public figure, this showing would ordinarily have required that the plaintiff demonstrate that the defendant had spoken with actual malice.[91] The court ruled that this element would be "difficult, if not impossible" to establish without access to the defendant's identity, and concluded that plaintiffs should be expected to demonstrate only the elements of their claim that relied upon knowledge of the defendant's identity.[92]

Another court considered a John Doe subpoena in 2007, after an anonymous Internet user obtained a copy of a salacious e-mail that a company CEO sent to his mistress and distributed it to company management personnel. The company, Mobilisa, sued for trespass to chattels, arguing that their computer systems must have been hacked to retrieve the e-mail, and subpoenaed the anonymous e-mail service that had been used to forward the e-mail, seeking the defendant's identity.[93] Although the central claim in *Mobilisa, Inc. v. Doe 1* was property-based, rather than speech-based, the court concluded that "the potential for chilling anonymous speech remains the same," and that, as a result, First Amendment concerns should remain central to its analysis.[94] The *Mobilisa* court expressly adopted *Cahill*'s notice and adverse summary judgment factors, but reintroduced a *Dendrite*-style balancing test factor that would allow revelation of the defendant's identity only if "a balance of the parties' competing interests favors disclosure."[95] Because the lower court had not properly considered this final balancing factor, the court remanded "for consideration of that step."[96]

In *Krinsky v. Doe 6*, the last John Doe subpoena standard that this Note considers, a corporate officer sued anonymous speakers for personal attacks against her on a message board.[97] *Krinsky* endorsed a *Cahill-Dendrite* standard,

89. *Id.* at 460-61.

90. *Id.* at 463.

91. *Id.* at 464.

92. *Id.*

93. Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 715-16 (Ariz. Ct. App. 2007).

94. *Id.* at 719.

95. *Id.* at 723-24. The question of whether John Doe subpoena standards should include a balancing test remains unresolved, and is addressed in more detail in Part III.F.

96. *Id.* at 724.

97. 72 Cal. Rptr. 3d 231 (Ct. App. 2008).

with two important distinctions. First, it noted that the defendant had already been notified by his ISP, making notice by the plaintiff largely of theoretical import.[98] Second, it concluded that a "summary judgment" standard was confusing and varied between jurisdictions. As a result, the court returned instead to the *Dendrite* terminology requiring "a prima facie showing of the elements of libel in order to overcome a defendant's motion to quash a subpoena seeking his or her identity."[99] The court concluded that the messages "did not constitute assertions of actual fact and therefore were not actionable under Florida's defamation law."[100]

These three cases demonstrate several important developments. First, their standards demand stronger showings of plaintiffs than the first four, and universally require defendant notice—a factor that, of the early cases, only *Dendrite* included. This suggests greater recognition by the courts of the unusual challenges posed by John Doe subpoenas. Second, they are more consistent than the earlier standards. Rather than varying across all six factors, they focus on only two: notice to the defendant and the strength of the plaintiff's argument.[101] This provides a perfect opportunity to examine the direction of John Doe subpoena doctrine before it develops into an entrenched consensus. Indeed, given the rapid changes to the online environment and the rise of online harassment, it is especially important to incorporate these developments into an analysis of John Doe subpoenas while the doctrine is still forming.

98. *See id.* at 244.

99. *Id.* at 245.

100. *Id.* at 251.

101. See table accompanying note 102 for a graphical representation of this phenomenon.

CASE[102]	NOTICE	STRENGTH OF ARGUMENT	RELEVANCE	SPECIFICITY	BALANCING TEST	EXHAUSTION
Seescandy.com (1999)[103]		X	X			X
In re AOL (2000)[104]		X	X	X		
Dendrite (2001)[105]	X	X	X	X	X	
2TheMart.com (2001)[106]		X	X			X
Cahill (2005)[107]	X	X				
Mobilisa (2007)[108]	X	X			X	
Krinsky (2008)[109]	X	X				

Before turning to close analysis of the factors that make up John Doe subpoena standards, however, there are two important concerns to consider regarding the standard that this Note will propose. First, the standard can govern the release of the identity of defendants and nonparty witnesses. *2TheMart.com* noted that the balance of First Amendment interests in exposing a nonparty witness differs from revealing the identity of a defendant—an "exceptional case" is necessary to justify exposing a nonparty witness.[110] The standard proposed below is flexible enough to incorporate these shifts, and this Note will indicate where these shifts would need to be considered.

102. This table shows the factors that each major John Doe subpoena standard includes.

103. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 579-80 (N.D. Cal. 1999).

104. *In re* Subpoena Duces Tecum to Am. Online, Inc. (*In re AOL*), 52 Va. Cir. 26, 37 (Cir. Ct. 2000).

105. Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super Ct. App. Div. 2001).

106. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

107. Doe No. 1 v. Cahill, 884 A.2d 451, 461-63 (Del. 2005).

108. Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 721 (Ariz. Ct. App. 2007).

109. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 244-45 (Ct. App. 2008).

110. Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001) ("[N]on-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker.").

Second, this standard should be applied only when the information sought by the plaintiff is sufficient to identify the defendant or nonparty witness. As noted previously, a plaintiff will often require two steps to identify an anonymous defendant.[111] Ensuring proper notice and opportunity to defend only against the final step protects defendants' First Amendment interests and prevents defendants from having two opportunities to mount the same defense. This is largely how John Doe subpoenas currently function, as services logging only IP addresses are usually unable to notify defendants.[112] As IP addresses become more directly traceable and new forms of online identification are deployed, the definition of information sufficient to positively identify the defendant will expand. So long as plaintiffs require multiple steps to identify defendants, however, the initial steps should not be governed by the standard proposed within this Note. An ordinary subpoena to the third-party service will be sufficient.

B. Notice and Opportunity To Respond

The first factor that many John Doe subpoena standards consider is whether the defendant was given notice and an opportunity to respond anonymously. If the defendant is not notified, the subpoena will only be challenged if the third party target of the subpoena moves to quash it on the defendant's behalf.[113] Although this is becoming a more common occurrence, it is certainly not universal. Without a challenge, the subpoena is reviewed ex parte and often complied with after little or no review. Because of the danger posed by unjustified discovery of a defendant's identity, it is important that defendants be informed and given an opportunity to contest their exposure.

An effective notice provision addresses three questions: Who should be required to notify? How should the defendant be notified? How long should the defendant have to respond? Each of these elements must be evaluated if a notice factor is to be properly balanced.

1. Who Should Be Required To Notify?

Both the plaintiff and the third-party target of the subpoena could be required to notify the defendant. Courts have thus far placed this burden on plaintiffs. *Dendrite* directed "the plaintiff to undertake efforts to notify the

111. *See supra* text accompanying note 27.

112. *See supra* note 86 and accompanying text.

113. *See, e.g.*, *In re AOL*, 52 Va. Cir. 26 (Cir. Ct. 2000).

anonymous posters that they are the subject of a subpoena."[114] *Cahill* and *Mobilisa* included almost identical requests that the plaintiff "undertake reasonable efforts to notify the anonymous defendant of the discovery request."[115]

Requiring that the plaintiff notify the defendant avoids encumbering the target of the subpoena—a third party that could easily be completely uninvolved in the events of the case. Because the plaintiff will often be unable to locate the defendant, however, requiring him to notify the defendant burdens him and does not ensure reliable notice.

No court as yet has required that the target of a subpoena notify the defendant. In some cases, however, ISPs are required by law to notify their clients before complying.[116] The Cable Communications Policy Act only allows cable company ISPs to release "personally identifiable information"[117] about their clients "if the subscriber is notified of such order by the person to whom the order is directed."[118] While there is no comparable federal law demanding notice by other types of ISPs, it is increasingly common practice for all ISPs to voluntarily notify their customers.[119] Considering these factors, *Krinsky v. Doe 6* concluded that "when ISPs and message board sponsors . . . themselves notify the defendant . . . notification by the plaintiff should not be necessary."[120] Lidsky has also suggested requiring third-party notice: "[S]ince [the] plaintiff will ordinarily seek the defendant's identity from an ISP, it is logical to require the ISP to give notice to its subscriber before disclosing the subscriber's identity."[121]

Because this standard applies only to subpoenas seeking identifying information,[122] the target of the subpoena will often be able to locate the defendant to notify him more effectively than the plaintiff could. If the target is unable to locate the defendant, a John Doe subpoena would be inappropriate,

114. Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

115. Doe No. 1 v. Cahill, 884 A.2d 451, 461 (Del. 2005); *see also* Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 719 (Ariz. Ct. App. 2007).

116. *See, e.g.*, *Cahill*, 884 A.2d at 455.

117. 47 U.S.C. § 551(c)(1) (2000).

118. *Id.* § 551(c)(2)(B).

119. *See, e.g.*, Roger M. Rosen & Charles B. Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, L.A. LAW, Oct. 2001, at 19, 19 ("Most ISPs now give their account holders two or more weeks' notice of a subpoena before divulging any information in response to it.").

120. 72 Cal. Rptr. 3d 231, 244 (Ct. App. 2008).

121. Lidsky & Cotter, *supra* note 16, at 1598.

122. *See supra* text accompanying note 111.

as the target would not have access to identifying information. At the same time, "[a]n ISP's primary interest is in minimizing cost and maximizing profit, not in protecting anonymous speech."[123] The commitment of ISPs and OSPs to protecting the identities of their customers is defined as much by business pressures as by a desire to preserve anonymous speech. The architecture of the Internet has already pressed them into the role of guardians of their customers' anonymity. Making them the sole source of notification would further cement them into a position for which they are at best imperfectly suited. Further, relying entirely on target notification of defendants would forego several collateral advantages of plaintiff notification, such as the increased public scrutiny that comes with publication notice.[124]

A comprehensive standard could mitigate this problem by requiring that both the plaintiff and the target of a subpoena attempt to notify the defendant. Indeed, Lidsky proposes just such a solution. In addition to recommending ISP notice to defendants, she also suggests that plaintiffs be required to notify defendants via publication.[125] This approach combines the benefits of notice by the plaintiff and notice by the target and ensures the greatest likelihood that defendants will receive notice. The burden on the target of the subpoena is mitigated because it will easily be able to locate the defendant to provide notice as the target must retain identifying information for this standard to apply.

2. How Should the Defendant Be Notified?

Next, the standard should indicate how the defendant is to be notified. There are at least three possibilities: direct notice, notice via the same method of communication that the defendant used for the actionable speech, and publication notice. Direct notice through some verifiable form of communication is the most certain form of notice. Plaintiffs can almost never accomplish direct notice, although targets of subpoenas, relying on client contact records, often can. Although courts have focused on indirect notice, having both plaintiffs and subpoena targets give notice would assure the defendant of both the certainty of direct notice and the benefits of the other forms of notice.

123. Orit Goldring & Antonia L. Hamblin, Note, *Think Before You Click: Online Anonymity Does Not Make Defamation Legal*, 20 HOFSTRA LAB. & EMP. L.J. 383, 396 (2003).

124. For more details on the advantages of notification by the plaintiff, see *infra* Subsection III.B.2.

125. Lidsky & Cotter, *supra* note 16, at 1598.

However it is served, the Court has held that notice must be "reasonably calculated, under all the circumstances, to apprise [the defendant] of the pendency of the action and afford [him] an opportunity to present [his] objections."[126] *Mullane v. Central Hanover Bank & Trust Co.* approved publication notice for defendants "whose interests or addresses are unknown to the trustee," but not for more directly reachable defendants.[127] Thus, the appropriate form of notice will vary from case to case.

Dendrite required that the plaintiff post "notification of the identity discovery request to the anonymous user on the ISP's pertinent message board."[128] This is an uncertain method of notice, as there is no way to ensure that the defendant will check the message board. Alternatively, if the defendant's speech occurred through e-mail, notice may be delivered to the originating e-mail address.[129] This is still unreliable, however, as there is no guarantee that the defendant will check the account.

Although publication notice may be the least reliable form of notice, it can be useful in the context of public speech because it informs the public as well as the defendant. This can call the veracity of the defendant's speech into question, allowing plaintiffs to begin to counter the damage of the speech without actually censoring it. Additionally, it puts the public on notice that the website or ISP has been subpoenaed. This scrutiny may compel the target to weigh the subpoena more carefully than it might if the subpoena were hidden from the public eye. Thus, publication notice carries important benefits beyond warning the defendant that a subpoena has been issued.

Of course, publication notice is only appropriate if the defendant's speech is published. Courts can require appropriate, effective notice for a given situation by tying it to the form of the speech in question. *Mobilisa* required that "[t]he requesting party's efforts must include notifying the anonymous party via the same medium used by that party to send or post the contested message."[130] Where the speech was public, such effort will require publication notice. Where private, they will require notice by the same channel as the original speech. This requirement prevents the plaintiff from claiming that some wildly inappropriate form of notice is sufficient and ensures the greatest likelihood of

126. United States v. Dusenbery, 223 F.3d 422, 424 (6th Cir. 2000) (holding that notice mailed to a prison inmate was sufficient for a forfeiture action) (citing Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950), which held that notice must reasonably convey the required information and afford sufficient opportunity for response).

127. 339 U.S. at 318.

128. Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

129. *See, e.g.*, Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 721 (Ariz. Ct. App. 2007).

130. *Id.* at 719.

notice to the defendant. Thus, while the form of notice will shift depending on the context of the particular case, an appropriate requirement would be that it be reasonably calculated to provide the defendant with timely warning, and effected through the same medium used by the defendant.

3. How Long Should the Defendant Have To Respond?

Finally, courts must determine how long defendants should have to respond anonymously to a subpoena seeking their identity. *Dendrite* includes a flexible time frame, requiring that the court should "withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition."[131] *Mobilisa* and *Cahill* both include similar requirements.[132] Some standards include explicit time limits,[133] and many ISPs that do notify their clients before complying with a subpoena have settled on two weeks as an appropriate time frame.[134] Nevertheless, it is difficult to apply a fixed requirement to the uncertainty of anonymous defendant notice. Because a defendant may not receive notice for days after the plaintiff gives it, the interests of the defendant suggest that a long response period would be most appropriate. At the same time, each moment that defamatory speech remains public can cause additional harm, so the plaintiff's interests suggest that the limit should remain short, at least for public speech. Given these competing pressures, a flexible "reasonable opportunity to respond" standard such as *Dendrite*'s seems most appropriate.

A flexible standard also fits with the reasonableness element presented in *Mullane*. It provides the defendant with a reasonable opportunity to respond, and the plaintiff with a reasonable chance to speedily remove the harmful speech. This flexibility should not be entirely unbounded, however. Courts should be suspicious of plaintiffs that provide defendants less than two weeks to respond. Although such a short window may be appropriate in extreme circumstances, it provides little opportunity for the defendant to mount a full defense and should require compelling justification.

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

132. *Mobilisa*, 170 P.3d at 719; Doe No. 1 v. Cahill, 884 A.2d 451, 461 (Del. 2005).

133. *See, e.g.*, CAL. CIV. PROC. CODE § 425.16(f) (West 2004) (giving the defendant sixty days to file a motion to quash a subpoena under California anti-SLAPP law).

134. *See* Rosen & Rosenberg, *supra* note 119, at 19.

4. An Appropriate Standard for Defendant Notice

Both the recipient of the subpoena and the plaintiff should make reasonable efforts to notify the defendant, including notice via the same medium used by the defendant to send or post the contested message. The defendant should be afforded a reasonable period to respond to the subpoena.

C. Strength of Plaintiff's Argument

The second key factor for evaluating a John Doe subpoena is the strength of the plaintiff's claim. It is the most commonly included element in John Doe subpoena standards—all but one of the seven standards considered in this Note include such a requirement.[135] The strength of argument that a plaintiff must demonstrate to unmask a defendant varies widely, however. Courts have required that plaintiffs' claims meet four different standards: good faith, motion to dismiss, a prima facie evidentiary showing, and summary judgment. This Section will examine each standard in turn.

1. Good Faith

Only one court has adopted a good faith standard—the weakest of the four standards considered here. *In re AOL* required only that the plaintiff demonstrate "a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where the suit was filed."[136]

Good faith provides no concrete standard for courts. According to *Krinsky*, "it offers no practical, reliable way to determine the plaintiff's good faith and leaves the speaker with little protection."[137] *Cahill* considered and rejected a good faith standard, noting that "[p]laintiffs can often initially plead sufficient facts to meet the good faith test . . . even if the defamation claim is not very strong, or worse, if they do not intend to pursue the defamation action to a final decision."[138] A good faith standard provides little if any protection for defendants. Because the unmasking of a defendant's identity can cause

135. Only *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001), does not have a strength-of-argument factor in its standard. The *2TheMart.com* standard is one of the most pro-plaintiff standards adopted by any court.

136. 52 Va. Cir. 26, 37 (Cir. Ct. 2000).

137. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 241 (Ct. App. 2008).

138. 884 A.2d 451, 457 (Del. 2005).

significant harm and deter other anonymous speakers from entering public debate, defendants deserve more than merely symbolic protection.

2. Survive a Motion To Dismiss

Several courts have required that plaintiffs demonstrate that their claim can survive a motion to dismiss. *Seescandy.com* required that the "plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss."[139] *Seescandy.com* likened this to "[t]he requirement that the government show probable cause[, which] is, in part, a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong."[140]

Seescandy.com was decided in federal court. *Bell Atlantic Corp. v. Twombly* recently clarified the federal motion to dismiss standard for antitrust cases and suggested that this standard might apply more broadly: a plaintiff can only survive a motion to dismiss in federal court if he produces factual allegations that are "enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true."[141] On its face, this standard seems to afford insufficient protection for defendants. Relief can be more than speculatively possible and still be a virtual impossibility. It may not be appropriate to risk the unjustified exposure of a defendant's identity if a plaintiff can meet only this standard.

Transforming this into a national standard also poses another problem: John Doe subpoenas arise not only in federal court but also in state courts across the country. The showing necessary for a plaintiff to survive a motion to dismiss varies from state to state. In a notice pleading state, for instance, "a complaint need merely set forth a short and plain statement showing the plaintiff is entitled to relief in order to survive a motion to dismiss."[142] Indeed, "any allegation that put[s] the opposing party on notice of the claim"[143] is sufficient in a notice pleading state, even if it is "vague or lacking in detail."[144] In states that do not have notice pleading, the standard could be more

139. 185 F.R.D. 573, 579 (N.D. Cal. 1999).

140. *Id.*

141. 127 S. Ct. 1955, 1965 (2007) (citation omitted) (ruling on the burden facing a plaintiff to overcome a motion to dismiss by the defendant).

142. Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

143. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 243 (Ct. App. 2008).

144. Doe No. 1 v. Cahill, 884 A.2d 451, 458 (Del. 2005) (quoting VLIW Tech., L.L.C. v. Hewlett-Packard Co., 840 A.2d 606, 611 (Del. 2003)) (internal quotation marks omitted).

substantial. *Lassa v. Rongstad*, decided by the Wisconsin Supreme Court, settled on a motion to dismiss standard instead of a more stringent summary judgment standard because the "silly or trivial libel claims" that would defeat a motion to dismiss in a notice pleading state would not survive in Wisconsin, which requires "particularity in the pleading of defamation claims."[145]

Relying on a motion to dismiss label to evaluate John Doe subpoenas would create an inconsistent, uncertain standard that varied not based on jurisdictions' rulings or the plaintiffs' substantive claims, but on procedural standards that were never intended to govern anonymous speech. John Doe subpoenas in different states would be measured against seemingly arbitrarily varying standards. As a result, a motion to dismiss requirement would likely lead to forum shopping and reduce the value of adopting a single nationwide standard.

Requiring that plaintiffs meet a motion to dismiss standard would create variation among jurisdictions tied neither to a jurisdiction's holdings on anonymous speech, nor to a plaintiff's substantive claim. Further, motion to dismiss standards in many jurisdictions would be insufficiently protective of defendants' interest in anonymity. As a result, a motion to dismiss standard is inappropriate for evaluating John Doe subpoenas.

3. Withstand a Motion for Summary Judgment

Another standard that several courts have adopted is what Michael Vogel calls a "'defensive' summary judgment standard."[146] In other words, the plaintiff must present a case strong enough to overcome a defendant's claim of summary judgment. In federal court, summary judgment is granted "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial."[147] Because the burden of proof rests on the plaintiff to establish his case, he must demonstrate prima facie support for each element of his case to defeat a summary judgment standard.

This standard provides a more specific, measurable level of protection for defendants. Like a motion to dismiss standard, however, the meaning of a summary judgment standard varies among state jurisdictions based on procedural, rather than substantive, analysis. The *Krinsky* court rejected both motion to dismiss and summary judgment standards for exactly this reason:

145. 718 N.W.2d 673, 687 (Wis. 2006).

146. Vogel, *supra* note 34, at 850.

147. Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

"We find it unnecessary and potentially confusing to attach a procedural label, whether summary judgment or motion to dismiss, to the showing required of a plaintiff seeking the identity of an anonymous speaker on the Internet."[148]

A federal summary judgment standard may provide a more appropriate level of protection to anonymous defendants than a motion to dismiss standard. The fact that it remains tied to a procedural label that varies across jurisdictions without regard to substantive concerns, however, means that it is still a flawed standard for John Doe subpoenas.

4. Establish a Prima Facie Case

Instead of relying on procedural standards, some courts have required plaintiffs to make a prima facie evidentiary showing of their claim in order to discover the defendant's identity. This is identical to a federal summary judgment standard and provides an important level of protection for anonymous defendants. Further, it avoids the jurisdictional variation problem of a procedural label. *Dendrite* relied on a prima facie standard, requiring that the "plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis."[149] *Krinsky*, which also required a prima facie showing from plaintiffs, defined prima facie evidence as "that which will support a ruling in favor of its proponent if no controverting evidence is presented. It may be slight evidence which creates a reasonable inference of fact sought to be established but need not eliminate all contrary inferences."[150] In other words, in addition to a demonstration of a legally reasonable claim, the plaintiff must also provide a strong factual case—absent defendant rebuttals, contrary facts, and affirmative defenses.

Prima facie standards do vary, both across substantive claims (a prima facie showing of libel is different from a prima facie showing of trademark infringement) and across jurisdictions (a prima facie showing of libel in one state may be different from a prima facie showing of libel in another state). Indeed, *In re AOL* rejected this standard for reasons that sound very similar to the concerns that were raised regarding motion to dismiss and summary judgment standards: "What is sufficient to plead a prima facie case varies from state to state and, sometimes, from court to court."[151] This variation, however,

148. 72 Cal. Rptr. 3d at 244.

149. 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

150. 72 Cal. Rptr. 3d at 245 n.14 (quoting Evans v. Paye, 37 Cal. Rptr. 2d 915, 925 n.13 (Ct. App. 1995)) (internal quotation marks omitted).

151. 52 Va. Cir. 26, 36 (Cir. Ct. 2000).

is not problematic in the same way that the variance of motion to dismiss and summary judgment standards is. What is required to make a prima facie showing of an element of a claim does not vary between jurisdictions or substantive areas of the law. Rather, the elements for which a plaintiff must make a prima facie showing of his claim varies. For example, a prima facie claim of libel in Florida requires that the plaintiff show that "the defendant published a false statement about the plaintiff to a third party and that the false statement caused injury to the plaintiff."[152] By contrast, in Delaware, proving libel requires the plaintiff to show that "1) the defendant made a defamatory statement; 2) concerning the plaintiff; 3) the statement was published; . . . 4) a third party would understand the character of the communication as defamatory[; and] 5) the statement is false."[153] The meaning of a prima facie showing does not differ among the jurisdictions; by contrast, the requirements that a plaintiff must satisfy to establish that showing vary.

Rather than subjecting parties to a procedural standard that was not designed to govern substantive law, this variation allows jurisdictions to express differences of opinion on First Amendment doctrine. This variation is not only an important expression of federalism, it is compelled by *Erie Railroad Co. v. Tompkins*: "Except in matters governed by the Federal Constitution or by Acts of Congress, the law to be applied in any case is the law of the State."[154]

Overall, a prima facie standard effectively balances the First Amendment interests of plaintiffs and defendants, compels plaintiffs to specifically assert their claims, and ensures meaningful variation reflecting jurisdictional disagreements on substantive law. It is the most appropriate standard to require plaintiffs to meet when seeking to unmask anonymous defendants.

5. The Problem of Elements That Are Beyond the Plaintiff's Control

Requiring that plaintiffs make a prima facie showing leaves one final stumbling block. As Michael Vogel has noted, providing prima facie support for a plaintiff's claim "will often depend dispositively on the identity of the defendant. . . . [T]he plaintiff will need to know the defendant's identity, and

152. *Krinsky*, 72 Cal. Rptr. 3d at 247 (citing Valencia v. Citibank Int'l, 728 So. 2d 330 (Fla. Dist. Ct. App. 1999)).

153. Doe No. 1 v. Cahill, 884 A.2d 451, 463 (Del. 2005). Because the plaintiff in *Cahill* was a public figure, the court also required that the plaintiff show actual malice on the part of the defendant to prove libel. *Id. New York Times Co. v. Sullivan* established this requirement nationally, so it does not vary among jurisdictions, but applies for all public figure plaintiffs. 376 U.S. 254, 279-80 (1964).

154. 304 U.S. 64, 78 (1938).

in all likelihood take the defendant's deposition, to meet that burden."[155] For instance, where the plaintiff is a public figure, he must show that the defendant acted with actual malice to prove a claim of defamation.[156] As Vogel notes, it is extremely difficult to make a prima facie showing of actual malice without knowledge of the defendant's identity.[157]

Several courts have addressed this concern by requiring merely that plaintiffs substantiate elements of their claims that are "within the requesting party's control—in other words, all elements not dependent upon knowing the identity of the anonymous speaker."[158] This removes the impossible burden from the shoulders of the plaintiff. At the same time, however, excusing the plaintiff from a prima facie showing of any element that relies on the defendant's identity weakens the defendant's protection for a number of potential claims. Often, as with defamation, this weakens the standard to which the plaintiff is held just when the law indicates the standard should be especially high. As a full prima facie standard provides too high a bar, and fully relieving plaintiffs of responsibility for elements beyond their control provides too low a bar, some intermediate standard seems necessary.

In Part II, this Note argued that public speech concerning public figures deserves special protection. This distinction can be effectively imported into John Doe subpoena standards by requiring public figure plaintiffs responding to public speech to meet some reduced showing of proof regarding elements beyond their control, but excusing private figure plaintiffs from this burden. This will distinguish between speech that is especially valued, and so should be protected at all costs, and speech—such as the harassment of private figures—that could chill more speech than it creates and rob the public sphere of valuable contributions.

6. Heightened Standard for Public Figure Plaintiffs

The only question remaining is what intermediate standard ought to be imposed on elements of claims concerning public speech brought by public figure plaintiffs that are beyond the plaintiffs' control. One author who has proposed a heightened standard of protection for political speech suggested a

155. Vogel, *supra* note 34, at 807-08.

156. *See Sullivan*, 376 U.S. at 279-80.

157. Vogel, *supra* note 34, at 807-08.

158. Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

standard that could be appropriate here.[159] Under his proposal, the plaintiff would only be able to discover a defendant's identity for political speech if he could "show that the defamatory language at issue was of such an egregious nature that the plaintiff" would likely be able to produce "evidence of actual malice at trial."[160] If this standard were applied only to elements beyond the plaintiff's control, it could represent an intermediate increase in the burden for public figure plaintiffs responding to public speech.

However, what constitutes particularly "egregious" speech is by no means clear. No guidance is provided regarding the context in which speech should be considered egregious. If egregiousness simply means vulgarity or outrageousness, then the standard does not seem appropriate. Although vile speech may make readers cringe, its vileness does not determine whether its speaker is culpable. Given that the standard was offered within the context of defamation, it could be that egregiousness refers to egregiously false or egregiously malicious. While this is more appropriate than simple vileness, however, what would constitute egregiously false remains unclear. Egregious maliciousness could mean that the defendant was particularly reckless and uncaring regarding the falsity of his statement. Requiring that the plaintiff meet this burden, however, seems tantamount to requiring a demonstration of actual malice. Thus, the "egregiousness" standard seems either unclear or no weaker than an ordinary prima facie showing.

Tellabs, Inc. v. Makor Issues & Rights, Ltd.,[161] a recent Supreme Court case concerning securities fraud, presents another possibility. Because abusive litigation is a problem in securities fraud (not unlike the challenges of John Doe subpoenas), the Private Securities Litigation Reform Act of 1995 (PSLRA) has "[e]xacting pleading requirements."[162] To establish securities fraud, the plaintiff must "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind."[163] A similar standard could be an appropriate intermediate requirement in the John Doe subpoena context: The plaintiff must state with particularity facts giving rise to a strong inference of each element of his claim that relies on the defendant's identity. This standard does not hinge on an uncertain term such as "egregiousness." As

159. Ryan M. Martin, Comment, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 U. CIN. L. REV. 1217 (2007).

160. *Id.* at 1243.

161. 127 S. Ct. 2499 (2007) (holding that a strong inference of the scienter required for securities fraud had not been established, and remanding for further consideration).

162. *Id.* at 2504.

163. 15 U.S.C. § 78u-4(b)(2) (2000).

a result, its requirements are more grounded, and the standard itself is less open to untethered judicial interpretation.

The strong inference standard also provides jurisprudential analysis that can be used to inform its meaning. In *Tellabs*, the Court concluded that "[t]o qualify as 'strong' . . . an inference . . . must be more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference . . . ."[164] In other words, to meet this standard, there must be no other reasonable inference that is more likely to be true than the plaintiff's claim.

This is certainly a more specific standard than the "egregiousness" standard. It imposes a significant burden, but only on public figure plaintiffs responding to public speech—the form of anonymous speech identified by courts as most deserving of protection. This distinction will make it possible for private targets of anonymous online speech to respond effectively while protecting the classic form of anonymous speech directed at public figures.

7. An Appropriate Standard for the Strength of the Plaintiff's Argument

Incorporating the public figure analysis from Part II results in a bifurcated standard that appropriately distinguishes between public and private online speech, demanding a higher burden of proof from public figure plaintiffs faced with public speech.

If the plaintiff is not a public figure, or the defendant's speech was not public, the plaintiff must produce prima facie support of all elements of the case within his control. If the plaintiff is a public figure responding to public speech, he must provide prima facie support for each element within his control and state with particularity facts giving rise to a strong inference of each element that is outside his control.

D. Relevance of Information Sought

A third factor of many John Doe subpoena standards is a requirement that the information sought by the plaintiff have some degree of relevance to the plaintiff's case. The degree of relevance required can vary widely, with the information sought needing to be anything from simply useful to vital to the plaintiff's claim. Shifting this bar will determine whether a plaintiff can use a John Doe subpoena to engage in a virtual fishing expedition based on suspicion, or whether he will be constrained to pursuing only leads that are reasonably supported prior to the John Doe subpoena.

164. 127 S. Ct. at 2504-05.

In re AOL required that "the subpoenaed identity information is centrally needed to advance [the plaintiff's] claim."[165] Cases involving journalists' protection of anonymous sources have also relied heavily on requiring that the information sought be central to the plaintiff's case. *Mitchell v. Superior Court*, for instance, required that a journalist could only be compelled to reveal his sources if their identities went "to the heart" of the plaintiff's claim.[166]

Similarly, *2TheMart.com* only allowed the release of information that was "directly and materially relevant to [a core] claim or defense."[167] In discussing this high standard, the court noted that "[u]nder the Federal Rules of Civil Procedure discovery is normally very broad, requiring disclosure of any relevant information that 'appears reasonably calculated to lead to the discovery of admissible evidence.' But when First Amendment rights are at stake, a higher threshold of relevancy must be imposed."[168] *2TheMart.com* paid particular attention to its relevancy requirement because the plaintiff sought the identity of nonparty witnesses in addition to defendants. When courts applying this Note's standard consider subpoenas for nonparty witnesses, they should be especially critical of information requests that are not central to the plaintiff's claim.

A relevancy requirement with a fairly high bar is an important element of any John Doe subpoena standard that seeks to protect defendants' First Amendment rights. Without a relevancy requirement, plaintiffs can use even a tangential claim as a reason to expose an anonymous speaker. *Dendrite* incorporates relevancy analysis into its balancing test factor.[169] Considering relevance separately, however, ensures that courts will explicitly consider the necessity of the information that the plaintiff seeks. This will limit the ability of ingenious plaintiffs to uncover and expose unnecessary, potentially embarrassing information about a defendant simply as a form of self-help, rather than as part of a larger legal claim.

One formulation of a standard that would address these concerns would be as follows: The plaintiff shall demonstrate that the information sought by subpoena is necessary for the identification of the defendant, and that the defendant's identity is central to the plaintiff's case.

165. 52 Va. Cir. 26, 37 (Cir. Ct. 2000).

166. 690 P.2d 625, 632 (Cal. 1984).

167. 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

168. *Id.* at 1096 (quoting FED. R. CIV. P. 26(b)(1)).

169. 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001).

E. Specificity of Crime and Evidence

Another factor that some courts have used to prevent plaintiffs from using unfounded allegations as a cover for a John Doe subpoena is to require specificity from the plaintiff. While courts have required specificity of evidence, specificity of information sought is also relevant. Both compel the plaintiff to produce detail, affording the court and the defendant an opportunity to examine and rebut questionable assertions. Both of these forms of specificity serve important roles. Both, however, can be incorporated into other factors without being adopted as independent elements themselves.

In re AOL and *Dendrite* both contain specificity of evidence requirements. *Dendrite* requires that the plaintiff "identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech."[170] Although *In re AOL* does not impose a similar requirement as part of its standard, its discussion directs the plaintiff "to produce the subject Internet postings, so that the Court [can] better determine whether there is, in fact, a good faith basis for [plaintiff's] allegations."[171] A specificity of evidence requirement ensures that plaintiffs clearly state the basis of their claims against defendants, providing some limited protection against John Doe subpoenas based on frivolous claims. *In re AOL*, which only requires that the plaintiff demonstrate a good faith claim, needs a specificity requirement because good faith does not require specificity. To meet the prima facie showing required by *Dendrite* and other more recent standards, however, a plaintiff must make a specific showing of his evidence.[172] Thus, for these higher bars, a separate specificity factor is not necessary. The *Cahill* court concluded that a specificity requirement was unnecessary because "[t]o satisfy the summary judgment standard a plaintiff will necessarily quote the defamatory statements in his complaint."[173] Since the standard proposed in this Note, like *Dendrite*, relies on a prima facie standard, no separate specificity of evidence requirement is necessary.

A specificity requirement should also be incorporated into another factor: the relevance of information sought. A clever plaintiff could use a broadly relevant search for the defendant's identity as cover to seek irrelevant, damaging, and embarrassing details about the defendant, such as websites he

170. *Id.*

171. 52 Va. Cir. 26, 37 (Cir. Ct. 2000).

172. *See, e.g.*, *Dendrite*, 775 A.2d at 760.

173. 884 A.2d 451, 461 (Del. 2005). *Cahill* refers to the *Dendrite* standard as a "summary judgment" standard, even though it is actually a prima facie standard.

visited or online services he used. Incorporating a requirement of specificity of information sought into the language adopted in the previous section will prevent this behavior. Instead of requiring only that "the plaintiff shall demonstrate that the information sought by subpoena is necessary,"[174] updated language would read: "The plaintiff shall demonstrate that each specific element of information sought by subpoena is necessary."[175] This addition will ensure that not only the defendant's identity, but also each piece of information sought by a John Doe subpoena, is needed to advance the plaintiff's claim.

One article advising plaintiff's lawyers in anonymous online speech cases recommends that "[t]he subpoena directed to the ISP should be broad in scope. It should ask for all ISP logs tracking the times, dates, and places of any offending postings by an anonymous poster as well as . . . the poster's name, address, and telephone number."[176] Requiring specificity will prevent overbroad discovery requests. A stand-alone specificity factor is unnecessary, however. Specificity elements can be incorporated into the strength-of-argument and relevance factors where appropriate. With this adjustment, a freestanding specificity factor is unnecessary.

F. Balancing the Rights of the Plaintiff and the Defendant

Another element that some courts have considered when evaluating John Doe subpoenas is an explicit balancing of plaintiffs' and defendants' interests. John Doe subpoenas arise with varied contexts, actors, and substantive claims and rely on rapidly developing technology. These shifting, unpredictable pressures make it very difficult to encapsulate all the factors a judge might need to consider. A flexible balancing factor would allow them to balance the varying First Amendment interests that will develop in John Doe subpoena cases.

Courts have used the balancing tests to incorporate considerations that were left out of the rest of their standard. *Sony Music Entertainment Inc. v. Does 1-40*, for instance, set the interests of the plaintiffs and defendants against each other through a specific inquiry into the defendants' expectation of privacy.[177] As the court concluded, "[D]efendants' First Amendment right to remain anonymous must give way to plaintiffs' right to use the judicial process to

174. *See supra* Section III.B.

175. For the full text of the updated factor, see *infra* Section IV.A.

176. Rosen & Rosenberg, *supra* note 119, at 19.

177. 326 F. Supp. 2d 556, 566-67 (S.D.N.Y. 2004).

pursue what appear to be meritorious copyright infringement claims."[178] Similarly, *Dendrite* instructs courts to "balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."[179] This incorporates both the value of the defendant's anonymous speech and the relevance of the information sought.

Cahill rejected *Dendrite*'s balancing test because "[t]he [balancing test] adds no protection above and beyond that of the summary judgment test and needlessly complicates the analysis."[180] In other words, if a plaintiff must demonstrate a claim that will survive a motion for summary judgment to discover a defendant's identity, the court must already balance the defendant's right to anonymous speech against the strength of the plaintiff's claim. The standard proposed in this Note requires a similar balancing as part of its prima facie standard. Although this does suggest that the specific balancing test outlined in *Dendrite* may be unnecessary, *Cahill* does not consider "whether balancing a broader range of competing interests is warranted."[181]

Mobilisa rejected *Cahill*'s elimination of the balancing test, concluding that there were other factors that should be considered in a balancing test, including "the type of speech involved, the speaker's expectation of privacy, the potential consequence of a discovery order to the speaker and others similarly situated, the need for the identity of the speaker to advance the requesting party's position, and the availability of alternative discovery methods."[182] Indeed, there are several elements that courts should consider as part of a broader balancing test. First, there should be some consideration of the potential consequences of a discovery order on the defendant. Few consequences would be severe enough to tip the scales in the defendant's favor, but the threat of bodily harm, or even death, would be one such example.[183] A balancing test also provides the court with an opportunity to consider whether the information sought relates to a defendant or only to a nonparty witness.

A balancing test can also raise concerns, however. Michael Vogel warns that a balancing test could swallow the entire standard: "In effect, the court acknowledges that, even if plaintiff has alleged a viable legal claim against the

178. *Id.* at 567.

179. 775 A.2d at 760-61.

180. 884 A.2d at 461.

181. Mobilisa, Inc. v. Doe 1, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

182. *Id.* (footnote omitted).

183. *See* Lidsky & Cotter, *supra* note 16, at 1601-02.

defendant . . . the court may still exercise discretion to stop the case in its tracks."[184] A balancing test does provide broad power to judges with less accountability than a more rigidly defined standard. To mitigate this danger but retain the flexibility of a balancing test, it should be applied when the court is faced with an especially close case. If applying the first three factors of this Note's standard does not lead a court to a clear conclusion, it can then turn to this balancing test to manage the technological or legal complexity that led to the uncertainty.

An appropriate balancing test factor would be as follows: If the first three factors do not yield a clear outcome, the court should balance the hardships and the relative First Amendment interests of the plaintiff and defendant, and give preference to whichever party bears the greater burden under this test.

G. Exhaustion of Alternatives

Finally, some John Doe subpoena standards require that the plaintiff demonstrate that he has exhausted all other means to identify the defendant. *Seescandy.com* required that the plaintiff "identify all previous steps taken to locate the elusive defendant."[185] Similarly, *2TheMart.com* required that the plaintiff show that "information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[186]

This requirement is an effort to ensure that plaintiffs will resort to John Doe subpoenas only when absolutely necessary. As such, it is unnecessary if the John Doe subpoena standard properly balances the interests of the plaintiff and defendant. If that is the case, then there is no need to press plaintiffs toward an alternate method of discovery. There will be no danger of them taking advantage of the defendants because the standard prevents it. It should be no surprise that *Seescandy.com* and *2TheMart.com* are relatively weak standards. These requirements that plaintiffs use John Doe subpoenas only as a last resort suggest that the courts were concerned about the balance between plaintiff and defendant and sought to limit the standards' application.

IV. A SINGLE STANDARD FOR JOHN DOE SUBPOENAS

Combining the factors listed above yields a single John Doe subpoena standard that prevents frivolous attempts to unmask defendants, balances the

184. Vogel, *supra* note 34, at 808.

185. 185 F.R.D. 573, 579 (N.D. Cal. 1999).

186. 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

concerns of plaintiffs and defendants, and incorporates a consideration of the First Amendment value of defendants' and plaintiffs' speech. This final Part articulates the full proposed standard, and then applies the standard to a recent controversy.

A. Identifying an Anonymous Defendant

The standard involves four elements. First, both the recipient of the subpoena and the plaintiff should make reasonable efforts to notify the defendant, including notice via the same medium used by the defendant to send or post the contested message. The defendant should be afforded a reasonable period to respond to the subpoena.

Second, the court should evaluate the strength of the plaintiff's argument. If the plaintiff is not a public figure, or the defendant's speech was not public, he must produce prima facie support of all elements of the case within his control. If the plaintiff is a public figure responding to public speech, however, he must provide a prima facie showing of each element within his control and state with particularity facts giving rise to a strong inference of each element that is outside his control. In evaluating this factor, the court must determine whether the plaintiff is a public figure. The court should be very cautious in declaring a plaintiff a public figure based only on online speech, and should not declare the plaintiff a limited-purpose or involuntary public figure unless his status is derived from events that took place before the speech that is at issue or he utilizes his public status to hold himself forth as an advocate beyond simply responding to the speech in question.

Third, the plaintiff shall demonstrate that each specific element of information sought by subpoena is necessary for the identification of the defendant, and that the defendant's identity is central to the continuation of the plaintiff's case. It is important to note that, as discussed above, both this and the previous factor include requirements of specificity, requiring detailed production from the plaintiff without imposing a fifth factor.

Fourth, if the first three factors do not yield a clear outcome, the court should balance the parties' interests, giving preference to the party whose hardships and First Amendment interests are greater.

This standard strengthens the two central factors of recent John Doe subpoena standards—notice and a prima facie showing by the plaintiff—by adding third-party notice and requiring an additional showing from public figure plaintiffs. In addition, it explicitly evaluates two factors that recent courts have preferred to consider implicitly. In addition to providing strong protection for most anonymous speech, the standard is also bifurcated—providing significantly stronger protection for speech that targets public

figures rather than private figures. This ensures that speech on matters of public concern—the center of public debate—is protected, while private targets of anonymous harassment will have an opportunity to expose their attackers.

B. Applying the Standard: AutoAdmit

The AutoAdmit case—*Doe I v. Individuals, Whose True Names Are Unknown*[187]—arises out of an anonymous online message board frequented by undergraduate and professional students, including law students.[188] In addition to discussions about law school, postings included a range of harsh, sometimes violent or threatening speech with racist and sexist themes.[189] The posts targeted active users and nonusers alike, calling them out by name and harassing, threatening, and mocking them.[190] Most of the targets were women, and the threats and harassment were frequently sexual, including wild claims and violent fantasies.[191] In 2007, two of the targets sued, alleging a series of claims ranging from defamation to copyright infringement.[192]

The plaintiffs' first response was not to file a lawsuit. According to the plaintiffs' brief, they first contacted the website administrators, asking that the postings be removed.[193] When this failed, they spoke out to the *Washington Post* and others, seeking to use public pressure and more speech to combat the alleged defamation.[194] When the plaintiffs did bring suit, one of their first steps was to seek discovery of the identity of their pseudonymous defendants through John Doe subpoenas.[195] One of the defendants (charged under the user name "AK47") filed a motion to quash the subpoena to his ISP.[196] The

187. No. 3:07-CV-909 (D. Conn. filed Nov. 8, 2007).

188. *See* AutoAdmit, http://www.autoadmit.com (last visited Oct. 27, 2008).

189. *See* Ellen Nakashima, *Harsh Words Die Hard on the Web*, WASH. POST, Mar. 7, 2007, at A1.

190. *See id.*

191. *See* Citron, *supra* note 10, at 10.

192. *See* Second Amended Complaint, *Doe I*, No. 3:07-CV-909 (D. Conn. Aug. 5, 2008), *available at* http://online.wsj.com/public/resources/documents/autoadmit.pdf. For more detail on the events leading up to the lawsuit, see Citron, *supra* note 10, at 10-14.

193. Second Amended Complaint, *supra* note 192, at ¶ 23; *see also* Jarret Cohen, Challenge to Reputation Defender (Mar. 15, 2007), http://www.autoadmit.com/challenge.to.reputation.defender.html.

194. *See* Nakashima, *supra* note 189.

195. Second Amended Complaint, *supra* note 192.

196. John Doe 21's Memorandum in Support of Motion To Quash Plaintiff's Subpoena, *Doe I*, No. 3:07-CV-909, 2008 U.S. Dist. LEXIS 48749 (D. Conn. June 13, 2008).

motion was denied.[197] Evaluating this motion to quash provides an excellent opportunity to examine how this Note's standard might be applied.

First, notice to the defendant was adequate. The plaintiffs posted "notice regarding the subpoenas on AutoAdmit in January of 2008,"[198] thus serving notice through the same medium as the speech. They posted notice on January 25,[199] and issued their subpoena on February 1.[200] On February 7, AT&T, the recipient of the subpoena, directly notified the defendant, giving the defendant until February 25, the subpoena's date of production, to respond with a motion to quash.[201] As a result, the defendant had one month from the date of notice by publication, and eighteen days from the date of direct notice by AT&T. Notice from the plaintiff and target reinforced each other, combining to ensure that the defendant had an appropriate opportunity to respond. In this case, defendant received notice, filing a motion to quash on February 25.[202]

Second, the standard requires an evaluation of the strength of the plaintiffs' argument. To do this, one must first determine whether the plaintiffs were private or public figures. The fact that the *Doe I* plaintiffs attempted to respond with more speech before resorting to litigation makes this analysis particularly difficult. Prior to becoming targets of online speech, the plaintiffs were both private figures. The court should determine if their response to the allegedly defamatory speech is sufficient to transform them into public figures. Analyzing this would require the court to answer two questions: First, is their public speech significant enough to transform them into public figures? Second, is the topic of their speech a public controversy, or is it a "matter of public concern merely to gossips"?[203] Under the limited framework that this Note proposes, the plaintiffs would likely only be considered limited-purpose public figures if they spoke out significantly on a public controversy, rather than simply responding to personal attacks.

In this case, the plaintiffs' comments during interviews were focused on their personal experiences.[204] This places them squarely in the context of

197. *Doe I*, 2008 U.S. Dist. LEXIS 48749, at *22.

198. *Id.* at *13.

199. *Id.* at *6 n.3.

200. *Id.* at *5.

201. Plaintiffs' Memorandum of Law in Support of Opposition to John Doe 21's Motion to Quash Plaintiff's Subpoena at 1, *Doe I*, No. 3:07-CV-909, 2008 U.S. Dist. LEXIS 48749.

202. *See Doe I*, 2008 U.S. Dist. LEXIS 48749, at *5-6.

203. Lorain Journal Co. v. Milkovich, 474 U.S. 953, 964 n.9 (1985) (Brennan, J., dissenting).

204. *See, e.g.*, Nakashima, *supra* note 189 ("'I didn't understand what I'd done to deserve it,' said the student. 'I also felt kind of scared because it was someone in my community who was

Firestone, suggesting that they did not become public figures.[205] In addition to these interviews, the plaintiffs were represented by Reputation Defender, a company that claims to "deliver CONTROL over how others are able to perceive you on the Internet."[206] The company attempted to pressure AutoAdmit to remove the allegedly defamatory speech, relying on news coverage and direct contact. Finally, one of the plaintiffs published a retrospective in a law journal describing her experience.[207] The article focuses primarily on the plaintiff's experiences as a target of online harassment,[208] but it also discusses possible legal and social solutions to the plaintiff's situation.[209] Thus, while it focuses on the experiences of one of the plaintiffs, it also engages the broader debate.

As noted above, it would have been very difficult for the plaintiffs to respond with more speech without at least some spillover into the broader question of online harassment.[210] Thus, the plaintiffs' speech does not necessarily make them public figures. Indeed, there are at least four reasons why a court would likely not find the plaintiffs to be limited public figures, despite their public speech. First, although the plaintiffs did reference the broader context of online harassment, their speech predominantly focused on their personal conflict, rather than an effort to thrust themselves into the forefront of the larger debate. Second, the *Hutchinson v. Proxmire* Court was unwilling to grant that academic articles, which reach only a "relatively small category of professionals," were sufficient to transform their author into a public figure.[211] Third, the plaintiffs spoke only a handful of times over a limited period, and then abruptly stopped even though the controversy continued. In *Time, Inc. v. Firestone*, "a few press conferences" were insufficient to transform the plaintiff into a public figure.[212] Here, the speech was similarly limited in both time frame and scope. Finally, the plaintiffs' public status was

threatening physical and sexual violence and I didn't know who.'"); Jeff Tyler, *Get Yourself a Little Online Privacy*, MARKETPLACE, Mar. 2, 2007, http://marketplace.publicradio.org/display/web/2007/03/02/an_online_identity ("People would bring that up to me in the interview. So when they did, I knew they had searched me on the Internet.").

205. *See supra* note 51 and accompanying text.

206. ReputationDefender, Company: About Us, http://www.ReputationDefender.com/company (last visited Oct. 27, 2008).

207. Article on file with author to preserve the plaintiff's anonymity.

208. *Id.*

209. *Id.*

210. *See supra* Section II.B.

211. 443 U.S. 111, 135 (1979).

212. 424 U.S. 448, 454 n.3 (1976).

created by the efforts of their anonymous assailants.[213] If the plaintiffs' efforts to respond to the allegedly defamatory attacks with more speech were to transform them into public figures, numerous targets in similar situations might be motivated to turn immediately to legal responses. This incentive would reduce public engagement online and induce targets to choose censorship over more speech—exactly the opposite of what would strengthen the public sphere.[214] These factors suggest that the plaintiffs' speech was neither significant enough to transform them into public figures nor focused on a public controversy. As a result, they were probably not transformed into limited-purpose public figures by the events leading up to their case.

Because the plaintiffs remained private figures, they had to produce prima facie support of only the elements of the case within their control. The court noted the applicable Connecticut standard for libel: "(1) Doe 21 published a defamatory statement; (2) the defamatory statement identified the plaintiff to a third person; (3) the defamatory statement was published to a third person; and (4) the plaintiff's reputation suffered injury as a result of the statement."[215] As none of these factors rely on the defendant's identity, the private figure plaintiffs would need to provide prima facie support for each of them. Given that prima facie evidence "may be slight evidence which creates a reasonable inference of fact sought to be established but need not eliminate all contrary inferences,"[216] the plaintiffs likely met this burden. Indeed, the Connecticut court also found that the plaintiffs had made a prima facie showing of their claims.[217]

Third, the court should evaluate the relevance of the information that the plaintiffs sought to their case. It is clear that the identity of the defendant was central to the continuation of the plaintiffs' case, as it could not proceed without a named defendant. Further, the plaintiffs sought only "the name, address, telephone number, and email address" of the defendant.[218] This is a limited set of information that is necessary for identifying the defendant.

Finally, if the first three factors do not yield a clear outcome, the standard directs the court to balance the First Amendment and privacy interests of the

213. *See* Perzanowski, *supra* note 43; *see also Proxmire*, 443 U.S. at 135; *supra* text accompanying note 54.

214. *See supra* Section II.B.

215. Doe I v. Individuals, Whose True Names Are Unknown, No. 3:07-CV-909, 2008 U.S. Dist. LEXIS 48749, at *17 (D. Conn. June 13, 2008).

216. Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 245 n.14 (Ct. App. 2008) (quoting Evans v. Paye, 37 Cal. Rptr. 2d 915, 925 n.13 (Ct. App. 1995)).

217. *Doe I*, 2008 U.S. Dist. LEXIS 48749, at *20.

218. *Id.* at *14.

plaintiffs and defendants. In this case, the court would not need to reach the balancing test, as the first three factors were tilted in favor of the plaintiffs. It is worth noting, however, that the balancing test would lean in favor of the plaintiff as well. The speech in question was exactly the sort of anonymous harassment that was discussed above, and anonymity in this case was as likely to chill speech as to protect it. Further, the defendant had no special fears of exposure that might outweigh what the plaintiffs already faced.

When applied to this motion to quash, the standard comes down on the side of the plaintiffs. The application provides an important reminder of how narrow the public/private figure distinction has become online, as the Internet brings public speech within everyone's grasp. To keep a balance of First Amendment interests online, courts will need to be cautious when designating speakers as public figures, and expect the distinctions between the two groups to continue to narrow.

CONCLUSION

The ability to speak anonymously is critical to the openness of the Internet. The loss of the right to anonymous speech online would be a grave blow to the vibrancy of the public sphere. At the same time, however, anonymity can foster vicious attacks, especially those that would be socially unacceptable in traditional public discourse. This phenomenon cannot be erased entirely—indeed, it should not be. The wholesale elimination of such unpleasant speech would necessarily encompass valuable, protected speech in its sweep. Nevertheless, the increasing complexity of the online environment demands standards that govern online speech with increasing nuance. By distinguishing between speech targeted at private and public figures, and by distinguishing speech on public controversies, the standard that this Note proposes would ensure heightened protection for the speech that is most beneficial to the public sphere while simultaneously providing the targets of anonymous harassment a balanced opportunity to unmask their attackers.