

UNMASKING “ANON12345”: APPLYING AN APPROPRIATE  
STANDARD WHEN PRIVATE CITIZENS SEEK THE  
IDENTITY OF ANONYMOUS INTERNET DEFAMATION  
DEFENDANTS

ERIK P. LEWIS\*

*To any individual who wishes to make defamatory statements, the Internet provides not only a forum and an audience, but also a cloak of anonymity. It can be difficult for a plaintiff in an Internet defamation case to obtain redress from an anonymous defendant. The obstacles to relief that exist under current law are particularly troubling when the victims of defamation are private individuals, because defamation has the potential to be most harmful to them. When defamation against public figures or business associations is posted online and memorialized in an Internet cache, it can instantly be lost in long lists of search results, but an Internet search for a name that is not well-known or common will likely return a short list of results so that even one negative comment stands out.*

*After providing background information about Internet defamation claims and First Amendment protections in the context of defamatory speech, the author presents three standards that courts have used to determine when it is appropriate to unmask an anonymous Internet defamation defendant. Next, the author analyzes the reasoning behind the Communications Decency Act, which shields Internet service providers from liability as publishers or speakers of a third party’s defamatory statement and generally leaves victims of Internet defamation with no cause of action against anyone but the individual poster. The author also examines the manner in which each approach to unmasking anonymous Internet defamation defendants strikes a balance between the First Amendment’s protection of anonymous speech and laws that prohibit defamation. The author then recommends that the standards for unmasking anonymous Internet defendants should be tiered according to whether the plaintiff is a public figure, a corporate entity, or a private individual.*

---

\* J.D. Candidate, University of Illinois College of Law, 2009. I would like to thank Beth Manzullo and Victoria Pambianco Ose for their edits.

## I. INTRODUCTION

The hiring partner of a major law firm has a choice between two exceptional summer candidates. Each has a comparable GPA, similar extracurricular activities, and relevant work experience. Unfortunately, there is only one slot left to fill the firm's summer class. In an attempt to distinguish the two candidates, the partner plugs each name into Google. The first search yields no results; the other generates links to multiple anonymous message board posts about the candidate's sexual activity, including unsubstantiated claims that the candidate has a sexually transmitted disease.<sup>1</sup> Some posts even state that they were written by the candidate.<sup>2</sup> With all else being equal, the hiring partner is much better off selecting the candidate whose name is not associated with any objectionable content, regardless of its veracity.<sup>3</sup>

This example illustrates the notion that few things are more important to individuals than their reputation. Gossip, false rumors, and innuendo can hinder all aspects of our lives, from interactions with colleagues and employers to relationships with family and friends.<sup>4</sup> Particularly troubling are situations in which harmful statements become immortalized through print and broadcast media, extending reputational harm throughout an individual's local community and, in some cases, across the country. Fortunately, when potentially defamatory statements are made public, the offended party generally has recourse in the courts by suing the individual making the false statement or the media facilitating the false speech. The Internet, however, has added a new wrinkle to this problem.<sup>5</sup> Once posted, the speech is readily available for the online world to read, but in many cases the speaker is nothing more than an anonymous username.<sup>6</sup> This makes it extremely difficult for the victim to hold the speaker accountable for alleged harms.

This Note examines the unique characteristics of defamation of character on the Internet. Part II examines First Amendment law and its application to defamatory speech against both public and private citizens. Part II then looks at how the First Amendment is applied to Internet

---

1. *Doe I v. Individuals*, 561 F. Supp. 2d 249, 250–52 (D. Conn. 2008); *see also* Ellen Nakashima, *Harsh Words Die Hard on the Web: Law Students Feel Lasting Effects of Anonymous Attacks*, WASH. POST, Mar. 7, 2007, at A1.

2. Nakashima, *supra* note 1. A Yale law student, surprised to learn she had no offers after summer associate recruiting season, later discovered that she was the subject of derogatory comments on a message board devoted to discussions about law school. *Id.* One participant in the discussion claimed to be the student, thus giving readers the impression that she was a willing participant in the salacious conversation. *Id.*

3. *Id.* A research survey noted that half of U.S. hiring officials use Internet searches when considering potential applicants, and one-third of results yield material used to deny the applicants a job. *Id.*; *see also* DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION* 190 (2007).

4. *See* SOLOVE, *supra* note 3, at 189.

5. *See* Allison Stiles, *Everyone's a Critic: Defamation and Anonymity on the Internet*, 2002 DUKE L. & TECH. REV. 0004, ¶ 8, <http://www.law.duke.edu/journals/dltr/articles/pdf/2002dltr0004.pdf>.

6. *Id.* ¶ 9.

speech generally and anonymous—and potentially defamatory—Internet speech specifically, particularly in light of a congressional statute that immunizes Internet service providers (ISPs) from liability for content published on their sites. Part III delineates Congress’s reasoning for immunizing ISPs and then examines the different standards reached by courts in allowing or denying disclosure of the identities of anonymous Internet defendants. Part IV questions whether the rights of defamed private citizens are properly considered within the existing statutory and common law framework. It concludes that these rights have been largely ignored in the current debate surrounding Internet defamation. Finally, it proposes a tiered system of unmasking standards that requires courts to first categorize the plaintiff seeking an anonymous defendant’s identity as a public figure, a business entity, or a private citizen. Part IV suggests that the existing obstacles for plaintiffs should remain in place for public figures and business entities, but that a relaxed standard is more appropriate for a private citizen whose interest in preventing online defamation is strictly the protection of a reputation not meant for the glare of the public spotlight.

## II. BACKGROUND

In addressing the issue of defamation on the Internet, it is important to understand the Supreme Court’s interpretation of the First Amendment in relation to character defamation. This Part discusses the First Amendment in this context and its relation to anonymous speech in general. Next, it discusses the legal issues surrounding an Internet defamation claim. Finally, it examines several of the key standards courts have used in determining whether an anonymous Internet defendant’s identity should be revealed for a pending defamation lawsuit.

### A. *The First Amendment and Defamatory Speech*

The near-impossible standard courts impose on plaintiffs seeking to identify anonymous Internet posters stems from several important First Amendment principles.<sup>7</sup> First and foremost, the Supreme Court holds that the First Amendment protects anonymous speech.<sup>8</sup> In fact, protecting anonymous speech exemplifies the First Amendment’s purpose to shield unpopular opinions from suppression and retaliation by main-

---

7. See *Best W. Int’l, Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at \*3 (D. Ariz. July 25, 2006).

8. *Id.* (citing *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995)). *McIntyre* overturned an Ohio statute that prohibited anonymous campaign literature, but the protections for anonymous speech are not limited to political speech. See *McIntyre*, 514 U.S. at 341–43 (explaining the protection provided for anonymous literary speech, as well as anonymous handbills urging consumer boycotts); 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, 1217 (2007).

stream society.<sup>9</sup> Thus, although protecting an anonymous speaker's identity could promote impermissible forms of speech, such as fraudulent statements during an election season,<sup>10</sup> the value of free speech is accorded greater weight than the dangers of its potential misuse.<sup>11</sup>

There are limitations, however, on the right to speak anonymously.<sup>12</sup> For instance, individuals who infringe copyrights cannot hide behind the First Amendment.<sup>13</sup> More importantly for this discussion, defamatory speech, anonymous or not, deserves no protection.<sup>14</sup> Although this might be a significant limitation on absolute freedom of expression, individuals seeking to curb negative comments through defamation lawsuits still face stringent First Amendment standards.<sup>15</sup>

Defamation is a tort, and liability hinges on proof that the alleged defamatory statement is false.<sup>16</sup> In the case of public officials, the Supreme Court held in *New York Times Co. v. Sullivan* that defamation plaintiffs must prove the speaker had actual malice when making the allegedly defamatory comments.<sup>17</sup> The Court defined actual malice as speaking with the knowledge that the statements made are false or speaking while recklessly disregarding the possibility that the speech could be false.<sup>18</sup> This standard was extended to public figures<sup>19</sup>—those who are not government officials but are thrust into the public spotlight because of their involvement in important public affairs or by virtue of their fame.<sup>20</sup>

In *Gertz v. Robert Welch Inc.*, the Supreme Court refused to extend the actual malice standard to defamation cases involving private individuals.<sup>21</sup> Recognizing that private citizens are more vulnerable to injury because they lack access to self-help remedies such as media outlets utilized by public figures, the Court held that states can individually define an appropriate liability standard for publishers and broadcasters of de-

---

9. *McIntyre*, 514 U.S. at 357 (“Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.” (citation omitted)).

10. *Id.* at 349.

11. *Id.* at 357; Martin, *supra* note 8, at 1224.

12. *Best W.*, 2006 WL 2091695, at \*3.

13. *S. Motor Carriers Rate Conference v. United States*, 471 U.S. 48, 55–56 (1985).

14. See *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942) (“[Defamatory statements] are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.”); Martin, *supra* note 8, at 1225.

15. See *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 281–82 (1964) (holding that public officials must show actual malice on the part of a defamation defendant).

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

17. 376 U.S. at 279–80.

18. *Id.* at 280.

19. See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 335 (1974) (citing *Curtis Publ'g Co. v. Butts*, 388 U.S. 130, 162 (1967)).

20. *Curtis Publ'g*, 388 U.S. at 164 (Warren, C.J., concurring).

21. See 418 U.S. at 345–46.

famatory speech involving private individuals.<sup>22</sup> The Court did, however, prohibit states from adopting a strict liability standard.<sup>23</sup> In addition, in cases lacking proof of actual malice, the Court restricted damages to compensation for actual injury.<sup>24</sup> To show actual injury, the plaintiff must prove that the defendant's defamatory speech held him up to contempt or scorn within his community or tended to impair his standing in the minds of a large segment of his community's population.<sup>25</sup>

### B. *The First Amendment and the Internet*

The advent of the Internet created a new tool for communication, dramatically changing public discourse through its ability to allow an increasingly diverse population to participate in public debate.<sup>26</sup> Its eventual ubiquity brought First Amendment jurisprudence into the digital age.<sup>27</sup> The Supreme Court, in *Reno v. ACLU*, ruled that online speech is no different from other forms of communication and should enjoy the same constitutional protection as traditional forms of speech.<sup>28</sup>

In so deciding, the Court recognized not only the rapid growth of online communication,<sup>29</sup> but also the Internet's ability to give voice and an audience to any individual, rather than only those with access to media outlets.<sup>30</sup> The Court concluded that there is no justification for limiting the level of First Amendment scrutiny applied to the Internet.<sup>31</sup> Rather, it presumed that the government's involvement in the regulation of online speech would more likely than not unnecessarily interfere with the Internet's growth.<sup>32</sup>

---

22. *Id.* at 347.

23. *Id.* (“[S]o long as they do not impose liability without fault, the States may define for themselves the appropriate standard of liability for a publisher or broadcaster of defamatory falsehood injurious to a private individual.”).

24. *Id.* at 349–50. The Court did not believe states had any substantial interest in securing private citizens gratuitous awards “far in excess of any actual injury.” *Id.* at 349. Actual harm could include “impairment of reputation and standing in the community, personal humiliation, and mental anguish and suffering.” *Id.* at 350.

25. *McMann v. Doe*, 460 F. Supp. 2d 259, 269 (D. Mass. 2006) (citing *Yohe v. Nugent*, 321 F.3d 35, 39–40 (1st Cir. 2003)).

26. *Doe v. Cahill*, 884 A.2d 451, 455 (Del. 2005).

27. *See Reno v. ACLU*, 521 U.S. 844 (1997).

28. *Id.* at 885.

29. *Id.* at 870 (citing a government statistic that 200 million users would be online by 1999).

30. *Id.* (“Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.”).

31. *Id.*

32. *Id.* at 885 (“As a matter of constitutional tradition, . . . we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression . . . outweighs any theoretical but unproven benefit of censorship.”).

### C. *Legal Implications of Defamation on the Internet*

Traditional defamation claims provide several distinct avenues for recourse.<sup>33</sup> The author of a libelous statement is an obvious defendant, but a defamation plaintiff can also sue primary publishers<sup>34</sup> and distributors<sup>35</sup> of such statements.<sup>36</sup> A plaintiff seeking judgment for defamation on the Internet, however, finds these traditional avenues closed, particularly when dealing with anonymous speech.<sup>37</sup>

#### 1. *The Communications Decency Act of 1996*

The primary impediment for an Internet plaintiff is the Communications Decency Act of 1996 (CDA), which provides that no ISP shall be treated as the publisher or speaker of any third-party statements.<sup>38</sup> Congress passed the CDA in response to a New York trial court ruling that an ISP could be held liable for defamation if it attempts to edit content created by third parties.<sup>39</sup>

The court held that, regardless of whether the ISP can be completely (or even partially) effective in its editing, its active utilization of technology and manpower to delete comments it considered offensive clearly demonstrated editorial control.<sup>40</sup> Through the CDA, Congress explicitly sought to overrule this decision,<sup>41</sup> finding that the Internet was an important and rapidly growing communication medium<sup>42</sup> that should be encouraged to develop,<sup>43</sup> in part through ISP editorial control without publisher liability.<sup>44</sup> Subsequent cases looked at the CDA and its legislative

---

33. See Cara J. Ottenweller, Note, *Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act*, 41 VAL. U. L. REV. 1285, 1296–99 (2007) (discussing other potentially liable parties in addition to the author of libelous statements in defamation suits).

34. Primary publishers are persons or organizations with editorial control over a publication. *Id.* at 1297.

35. Distributors do not directly publish materials, but simply deliver or transmit materials published by third parties. *Id.* at 1298.

36. See *id.* Courts generally immunize a third category of potential defendants—conduit entities such as telephone or cable companies—due to a lack of control over the libelous content published or transmitted. *Id.*

37. See Thomas G. Ciarlone Jr. & Eric W. Wiechmann, *Cybersmear May Be Coming to a Website near You: A Primer for Corporate Victims*, DEF. COUNS. J., Jan. 2003, at 51, 59.

38. 47 U.S.C. § 230(c)(1) (2006).

39. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. (BNA) 1794, 1796–99 (N.Y. Sup. Ct. 1995); see also Sean P. Trende, *Defamation, Anti-SLAPP Legislation, and the Blogosphere: New Solutions for an Old Problem*, 44 DUQ. L. REV. 607, 621–24 (2006).

40. *Stratton*, 23 Media L. Rep. (BNA) at 1796–99.

41. Trende, *supra* note 39, at 623–24 (discussing the legislative debates leading to the CDA's passage).

42. 47 U.S.C. § 230(a).

43. *Id.* § 230(b).

44. *Id.* § 230(c)(1); see also Trende, *supra* note 39, at 624.

history and broadly interpreted it to immunize ISPs from distributor liability as well.<sup>45</sup>

Congress and the courts have created a major obstacle to justice for plaintiffs wronged by the tort of defamation. Anonymity on the Internet is as simple as creating a fake screen name on a site of the user's choice and posting away.<sup>46</sup> Although this can be viewed as positive and liberating to some,<sup>47</sup> there are drawbacks.<sup>48</sup> Hidden behind a cloak of anonymity, posters might use language in ways that they would never choose to speak in public, or even privately with close friends.<sup>49</sup> Anonymity also makes lying easier.<sup>50</sup> By immunizing ISPs when anonymous speech veers into the realm of defamation, Congress and the courts stripped plaintiffs of a viable defendant and forced them to seek recourse exclusively against the anonymous posters.<sup>51</sup> Unfortunately, the immunization of ISPs serves as another major hurdle for plaintiffs.

## 2. *Internet Defamation Lawsuits Involving Anonymous Defendants*

Due to the necessity of proving the speaker's actual malice (for public figures)<sup>52</sup> or negligence (for private citizens)<sup>53</sup> in making the defamatory statement, identifying the anonymous defendant is paramount. Proof would be next to impossible without a named defendant, as our adversary system relies on the discovery process—and resultant evidence—to bolster many claims.<sup>54</sup> Thus, plaintiffs face the difficult choice of deciding whether the significant front-end litigation costs of an ano-

---

45. See, e.g., *Ben Ezra, Weinstein, & Co. v. Am. Online, Inc.*, 206 F.3d 980, 986 (10th Cir. 2000); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 332–33 (4th Cir. 1997); *Trende*, *supra* note 39, at 624–29.

46. See *Martin*, *supra* note 8, at 1220 (“Overall, the internet seems to foster anonymity.”).

47. See *id.* (discussing the role Internet anonymity plays in fostering communication across race, class, gender, and other distinctions).

48. See, e.g., Kim Martineau, *Women Fight Web Smears*, HARTFORD COURANT, June 15, 2007, at A1 (reporting the case of two Yale law students whose real names were posted—along with lurid personal attacks—by anonymous users of an Internet message board).

49. See *SOLOVE*, *supra* note 3, at 140 (“When anonymous, people are often much nastier and more uncivil in their speech. It is easier to say harmful things about others when we don't have to take responsibility.”); see also *Ciarlone & Wiechmann*, *supra* note 37, at 62 (“Because the Internet is a virtual costume ball—with the identities of its millions of guests hidden behind masks of an intangible sort—the perceived anonymity of online speech lulls many into a false sense of invincibility.”).

50. See *SOLOVE*, *supra* note 3, at 140–41. When people spreading false rumors are discovered, their own reputation suffers. *Id.* The inability to identify those making false speech anonymously thus prevents this form of reputational deterrence. *Id.* at 141.

51. See *Lyrissa Barnett Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 872 (2000).

52. *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 279–80 (1964).

53. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 347 (1974) (prohibiting states from imposing strict liability as a standard for defining defamation involving private citizens). Following *Gertz*, most states adopted a negligence standard in defamation lawsuits brought by private individuals. See Michael Eric Johnston, *A Better SLAPP Trap: Washington State's Enhanced Statutory Protection for Targets of "Strategic Lawsuits Against Public Participation,"* 38 GONZ. L. REV. 263, 268 (2003) (citing *Rosner v. Field Enters., Inc.*, 564 N.E.2d 131, 141–42 & n.4 (Ill. App. Ct. 1990)).

54. See *Best W. Int'l, Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at \*4–5 (D. Ariz. July 25, 2006).

nymous Internet defamation lawsuit are worth the expense, particularly when the revelation of the poster's identity could lead the plaintiff to conclude that an actual defamation suit is not worth pursuing.<sup>55</sup>

If the plaintiff nevertheless decides to sue an anonymous Internet defendant, the civil procedure in such a suit will assume unique characteristics.<sup>56</sup> Lacking the ability to serve a proper defendant, a plaintiff generally will file suit against "John Doe" and then seek leave to subpoena Doe's ISP for Doe's identity.<sup>57</sup> This procedure can raise potential jurisdictional issues if the plaintiff chooses to file suit in federal court based on diversity of citizenship.<sup>58</sup> If a federal court determines that John Doe should be unmasked, diversity would be defeated if the ISP reveals that Doe and the plaintiff are residents of the same state.<sup>59</sup>

If a plaintiff can show good cause for issuing the subpoena, an anonymous defendant can fight the order through her attorney while remaining anonymous.<sup>60</sup> At this point, courts will usually hold a hearing to decide whether Doe's cloak of anonymity should be removed, weighing the defendant's First Amendment rights against the plaintiff's interest in rectifying perceived defamation.<sup>61</sup>

#### D. Approaches to Unmasking Anonymous Internet Defendants

Courts have varied widely in adopting an appropriate standard for unmasking anonymous defendants.<sup>62</sup> It is a decision with important constitutional considerations, and courts therefore must choose a "standard such that aggrieved parties can obtain remedies, but can not demand the court system unmask every insolent, disagreeable, or fiery anonymous online figure."<sup>63</sup>

Two similar standards have developed in response to the balance of competing interests in Internet defamation cases. The summary judgment standard, first articulated by the Delaware Supreme Court in *Doe v. Cahill*, is the most recent, and courts in several other jurisdictions have

---

55. See Stiles, *supra* note 5, ¶ 9. For example, a judge defamed by someone she sentenced to prison might deem a lawsuit unworthy of her time or money, as it would be obvious to the world that the speaker simply has a grudge against her, and a lawsuit would do little to vindicate her rights. *Id.*

56. Martin, *supra* note 8, at 1227.

57. See, e.g., *McMann v. Doe*, 460 F. Supp. 2d 259, 262–63 (D. Mass. 2006) (describing this discovery process undertaken by plaintiff Paul McMann); *Doe v. Cahill*, 884 A.2d 451, 454 (Del. 2005).

58. See *McMann*, 460 F. Supp. 2d at 263–65. Defamation is a tort governed by state law, and plaintiffs would thus have to rely on diversity jurisdiction when bringing defamation claims in federal court. See *id.*

59. *Id.* at 264.

60. See Martin, *supra* note 8, at 1227.

61. *McMann*, 460 F. Supp. 2d at 266; see also Martin, *supra* note 8, at 1227.

62. See Martin, *supra* note 8, at 1227–37.

63. *McMann*, 460 F. Supp. 2d at 266.

adopted or approved it.<sup>64</sup> The standard was derived from and shares elements of the motion to dismiss standard established in *Dendrite International, Inc. v. Doe*, a New Jersey appellate court decision that has also been cited with approval by other jurisdictions.<sup>65</sup>

### 1. *The Motion to Dismiss Standard*

In *Dendrite*, John Doe posted several comments on a Yahoo! message board specifically about Dendrite, a publicly traded New Jersey corporation, and its stock performance.<sup>66</sup> Doe was critical of the corporation's direction and changes to its revenue recognition accounting.<sup>67</sup> Dendrite filed suit against Doe, alleging that the postings constituted actionable defamation, and sought an order to show cause why Doe should not be identified.<sup>68</sup>

The *Dendrite* court articulated a four-step process for trial courts to follow when faced with an order compelling an ISP to disclose the identity of anonymous Internet posters: (1) require the plaintiff to notify defendants that they are the subject of a subpoena and withhold action until they have a reasonable amount of time to respond; (2) require the plaintiff to identify the exact defamatory statements; (3) require the plaintiff to set forth in his complaint a prima facie cause of action that can survive a motion to dismiss for failure to state a claim, as well as evidence supporting each element of the cause of action; and (4) balance the defendant's First Amendment rights against the strength of the plaintiff's case.<sup>69</sup>

### 2. *The Summary Judgment Standard*

In *Cahill*, Councilman Patrick Cahill filed suit against four John Doe defendants in response to defamatory statements on an Internet blog regarding his performance as councilman in Smyrna, Delaware.<sup>70</sup> The statements at issue questioned Cahill's leadership abilities and stated that Cahill suffered from mental illness.<sup>71</sup> One of the four anonymous

---

64. *Doe v. Cahill*, 884 A.2d 451 (Del. 2005); *see, e.g.*, *Best W. Int'l, Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at \*4 (D. Ariz. July 25, 2006); *Reunion Indus. Inc. v. Doe 1*, 80 Pa. D. & C.4th 449, 456 (Ct. Com. Pl. 2007).

65. 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *see, e.g.*, *Greenbaum v. Google, Inc.*, 845 N.Y.S.2d 695, 698 (N.Y. Sup. Oct. 23, 2007).

66. 775 A.2d at 761-63.

67. *Id.* at 763.

68. *Id.*

69. *Id.* at 760.

70. *Doe v. Cahill*, 884 A.2d 451, 454 (Del. 2005).

71. *Id.* One John Doe, under the alias "Proud Citizen," posted:

If only Councilman Cahill was able to display the same leadership skills, energy and enthusiasm toward the revitalization and growth of the fine town of Smyrna as Mayor Schaeffer has demonstrated! While Mayor Schaeffer has made great strides toward improving the livelihood of Smyrna's citizens, Cahill has devoted all of his energy to being a divisive impediment to any kind of cooperative movement. *Anyone who has spent any amount of time with Cahill would be keenly*

defendants appealed the Delaware Superior Court's ruling ordering Doe's ISP to disclose his identity.<sup>72</sup> The Delaware Supreme Court considered the various standards it could impose and expressed concern about setting the bar too low for plaintiffs, thus chilling potential posters from exercising their constitutional right to speak anonymously.<sup>73</sup>

After review of the *Dendrite* test, the court settled on a two-part summary judgment standard.<sup>74</sup> First, the plaintiff must post notice of his discovery request on the message board where the allegedly defamatory statement was originally posted.<sup>75</sup> Then, before a plaintiff alleging defamation is granted leave to discover an anonymous defendant's identity, he must support his claim with sufficient facts to defeat a motion for summary judgment.<sup>76</sup>

The *Cahill* court ignored the second and fourth prongs of the *Dendrite* test.<sup>77</sup> It argued that the second prong would be "subsumed in the summary judgment inquiry" because the plaintiff would necessarily have to quote the relevant statements to survive a defendant's motion for summary judgment.<sup>78</sup> The court rejected the fourth prong on the basis that it added an additional and unnecessary complication to the summary judgment analysis.<sup>79</sup> Essentially, surviving summary judgment would require the plaintiff to show he has a defamation case of some merit, and thus the judge would have already determined that the plaintiff's case outweighs the defendant's First Amendment rights.<sup>80</sup>

### 3. *The Good Faith Basis Standard*

Prior to the *Dendrite* and *Cahill* decisions, the Virginia Circuit Court established a "good faith basis" standard that has not gained much traction in other courts.<sup>81</sup> In *In re Subpoena Duces Tecum to America Online, Inc.*,<sup>82</sup> the court was asked to decide whether ISP America Online (AOL) should be forced to reveal the identity of five John Does.<sup>83</sup> An anonymous company filed suit against the Does for allegedly defamatory

---

*aware of such character flaws, not to mention an obvious mental deterioration.* Cahill is a prime example of failed leadership . . . .

*Id.*

72. *Id.* at 454–55.

73. *Id.* at 457.

74. *Id.* at 460–61.

75. *Id.*

76. *Id.* at 460.

77. *Id.* at 461.

78. *Id.*

79. *Id.*

80. *See id.*

81. *In re Subpoena Duces Tecum to Am. Online, Inc.*, No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000); *see, e.g.*, *Cahill*, 884 A.2d at 458. The Delaware Supreme Court overturned the superior court's decision adopting the good faith standard and holding that Doe's identity should be revealed. *Id.* at 455.

82. 2000 WL 1210372, at \*1.

83. *Id.*

statements about the company made in AOL chat rooms.<sup>84</sup> The plaintiff corporation served AOL with a discovery subpoena, and AOL sought to quash the subpoena on First Amendment grounds.<sup>85</sup>

The Virginia Circuit Court held that an ISP should be ordered to unmask an anonymous defendant only when (1) the court is satisfied by the pleadings or evidence presented; (2) that “the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed”;<sup>86</sup> and (3) the defendant’s identity is necessary for the plaintiff to advance his claim.<sup>87</sup>

At least one commentator has noted that the court never defined “good faith basis” as it applies in a defamation claim<sup>88</sup> and argues for its abandonment in Internet defamation jurisprudence.<sup>89</sup> In addition, the *Cahill* court rejected this standard because it is too easily met by plaintiffs to sufficiently protect a defendant’s right to speak anonymously.<sup>90</sup> It also lacks a notice requirement, which has become the norm in subsequent unmasking standards.<sup>91</sup> Due to the important First Amendment principles involved, one commentator argues that defendants should have an opportunity to respond and fight the subpoena.<sup>92</sup>

### E. Summary

This Part illustrates some of the key issues surrounding defamation and anonymous speech on the Internet. To understand why courts must consider a plaintiff’s status as a public figure, corporation, or private citizen when faced with a request for an anonymous defendant’s identity, Part III closely examines the CDA and the current standards courts utilize in such situations.

## III. ANALYSIS

There is no clear consensus amongst the courts regarding which standard to apply when asked to identify an anonymous defamation de-

---

84. *Id.*

85. *Id.*

86. *Id.* at \*8.

87. *Id.*

88. Martin, *supra* note 8, at 1228.

89. *Id.* at 1240–42.

90. Doe v. Cahill, 884 A.2d 451, 458 (Del. 2005); *see also* Krinsky v. Doe 6, 159 Cal. Rptr. 3d 231, 241 (Ct. App. 2008) (“[I]t offers no practical, reliable way to determine the plaintiff’s good faith and leaves the speaker with little protection.”).

91. *Cahill*, 884 A.2d at 460–61; Dendrite Int’l, Inc. v. Doe, 775 A.2d 756, 760 (N.J. Super. Ct. App. Div. 2001); *see also* Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 339–43 (2008) (compiling recent unmasking cases, which show a shift toward a notice requirement from earlier cases without such a requirement).

92. Gleicher, *supra* note 91, at 345.

fendant on the Internet.<sup>93</sup> This can create confusion for courts hearing Internet defamation claims for the first time.<sup>94</sup> In order to bring some semblance of clarity to the confusion, it is important to understand why this confusion exists. This Part first addresses the reasoning behind the passage of the CDA and its subsequent judicial interpretation. It explains that the leading interpretation of the CDA immunizes ISPs from defamation lawsuits and thus forces plaintiffs to seek restitution from the individual anonymous posters. Finally, this Part examines the reasoning behind each court's respective standard for unmasking anonymous Internet defendants in defamation suits.

#### A. *The CDA's Purpose and Subsequent Effect*

As discussed above, Congress passed the CDA in response to the *Stratton* decision in 1995.<sup>95</sup> The court held the ISP in that case liable for defamation as a publisher after the ISP assumed editorial control over certain content on its message boards, in part to market itself as "family-oriented."<sup>96</sup> Congress was concerned that this decision might disincentivize ISPs from self-regulating content for fear that assuming such control would open themselves up to potential defamation liability.<sup>97</sup> With the Internet rapidly developing, Congress did not want to see that development hindered.<sup>98</sup> Families in particular might be reluctant to adopt Internet usage if ISPs decided it would be easier to allow indecent content on their sites than to take steps to eliminate such content.<sup>99</sup> Thus, Congress passed the CDA with two important provisions.<sup>100</sup> First, no ISP would "be treated as a publisher or speaker" of third-party content.<sup>101</sup> Second, no ISP would incur civil liability for taking voluntary action in

---

93. See discussion and cases cited *supra* Part II.D.

94. See, e.g., *Essent v. Doe*, Citizen Media Law Project, <http://www.citmedialaw.org/threats/essent-v-doe> (last visited Apr. 5, 2009). *Essent* Healthcare sued an anonymous blogger for defamation, among other claims. It filed an order to compel the blogger's ISP to reveal his identity, and the district court judge quotes three different standards in a letter compelling disclosure but does not identify the standard he relied on to make his ruling. See *id.* The district court ruling was subsequently overturned, and the *Cahill* summary judgment standard adopted, by a Texas appellate court. See *In re Does 1-10*, 242 S.W.3d 805, 815-16 (Tex. App. 2007).

95. See discussion *supra* Part II.C.1.

96. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. (BNA) 1794, 1795 (N.Y. Sup. Ct. 1995).

97. See *Ottenweller*, *supra* note 33, at 1301.

98. See 47 U.S.C. § 230(b)(1) (2000) ("It is the policy of the United States . . . to promote the continued development of the Internet and other interactive computer services and other interactive media[.]").

99. See *id.* § 230(b)(4) ("It is the policy of the United States . . . to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.").

100. *Id.* § 230(c).

101. *Id.* § 230(c)(1).

restricting access to or availability of certain materials,<sup>102</sup> thereby allowing the editorial control in *Stratton* without the legal liability.<sup>103</sup>

After the CDA's passage, courts interpreted it more broadly than simply immunizing ISPs from publisher liability.<sup>104</sup> The Fourth Circuit, in *Zeran v. America Online, Inc.*, noted that "[i]f computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement."<sup>105</sup> Thus, if an ISP were liable on notice, it would be easier for the ISP to simply erase any questionable comments, as the large volume of Internet postings would make investigation and self-policing nearly impossible.<sup>106</sup> This would likely chill Internet speech.<sup>107</sup> The court thus held that the CDA immunizes both publisher and distributor liability.<sup>108</sup>

Not everyone believes *Zeran* is the correct interpretation of the CDA.<sup>109</sup> A dissenting opinion by the Florida Supreme Court in *Doe v. America Online, Inc.* questioned the *Zeran* decision.<sup>110</sup> By looking at the plain language of the statute, the dissent argued that Congress intended to immunize ISPs only from publisher liability when they sought to implement self-regulating policies.<sup>111</sup> Nothing in the language of the statute suggests immunization from distributor liability as well, otherwise Congress would not have included "publisher or speaker" in the statute.<sup>112</sup> Further, it would make little sense for Congress to pass an act promoting decency on the Internet by encouraging ISP self-policing efforts if an ISP could instead choose to do no self-policing when notified of harmful content and remain free of liability.<sup>113</sup> Instead, the more likely intent of Congress was to immunize ISPs that actively review and edit inappropriate content while leaving others vulnerable to lawsuits if they "do *not* screen any third-party content whatsoever."<sup>114</sup>

Several commentators support the dissent's interpretation.<sup>115</sup> The CDA could be read to grant immunity only until the ISP is informed of defamatory speech on its Web site.<sup>116</sup> Once informed, the ISP is aware of

---

102. *Id.* § 230(c)(2).

103. See Ottenweller, *supra* note 33, at 1301, 1303.

104. See cases cited *supra* note 45.

105. 129 F.3d 327, 333 (4th Cir. 1997).

106. *Id.*

107. *Id.*

108. *Id.*; see also Ottenweller, *supra* note 33, at 1307.

109. Ottenweller, *supra* note 33, at 1307.

110. 783 So. 2d 1010, 1018–28 (Fla. 2001) (Lewis, J., dissenting).

111. *Id.* at 1024.

112. *Id.* at 1025.

113. *Id.* at 1024–25.

114. Chi. Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 681, 697 (N.D. Ill. 2006).

115. See, e.g., SOLOVE, *supra* note 3, at 154–60; Ottenweller, *supra* note 33, at 1317–34. Solove notes that broad immunity for ISPs fosters irresponsibility and allows less than reputable Web sites that post gossip and rumors to thrive. SOLOVE, *supra* note 3, at 260.

116. See SOLOVE, *supra* note 3, at 154.

a potential problem, and doing nothing about the problem constitutes an implicit endorsement of the comment for which the ISP should be held liable.<sup>117</sup> Thus, Congress should amend the CDA to emphasize protection from publisher liability only.<sup>118</sup> The amendment should also include a subsection explicitly providing that an ISP is not immune from distributor liability if it has notice of objectionable material and fails to take remedial action.<sup>119</sup>

Alternate interpretations and calls for explicit amendments allowing distributor liability have a certain surface appeal. When a defamation plaintiff discovers harmful content posted on the Internet and requests that an ISP remove it, it appears fair to hold the ISP responsible for defamation when it refuses to remove that content. After all, a bookstore that refuses to remove defamatory content from its inventory can be held liable for defamation upon notice of the libelous material for sale on its shelves.<sup>120</sup> Distributor liability also virtually guarantees a plaintiff a viable defendant in a defamation suit in which the poster is anonymous, provided the plaintiff puts the ISP on notice and the ISP takes no action. Thus, even in cases in which the requirements of various unmasking standards cannot be met, a plaintiff still has the opportunity to rectify alleged harms by holding the site accountable for contributing to the harm through inaction.<sup>121</sup>

The problem with an alternate interpretation of or explicit amendment to the CDA, as the *Zeran* court articulates, is that subjecting ISPs to liability on notice of potentially defamatory content can lead to wholesale deletion of said content, regardless of whether it truly rises to the level of defamation.<sup>122</sup> Critics of the *Zeran* decision fail to consider the precarious role into which an ISP would be forced. Though some defamation cases are relatively easy to identify, many hinge on the dreaded case-by-case determination. An ISP cannot always determine with relative certainty whether a comment rises to the level of defamation, and some may believe in the promotion of unregulated speech.<sup>123</sup> When faced with the expense of a potential defamation lawsuit, it becomes much easier for an ISP to justify deleting borderline comments rather than fighting a lawsuit on principle.<sup>124</sup> Some critics seemingly ignore this problem by noting that defamation is not entitled to First Amendment

---

117. *Id.*

118. See Ottenweller, *supra* note 33, at 1329.

119. *Id.* at 1326–28.

120. *Id.* at 1298.

121. *Id.* at 1333–34. This is not to suggest that the speaker should be unaccountable; rather, when tracking down the anonymous speaker yields little to no information, the harm to the plaintiff can still be rectified by holding the ISP accountable.

122. *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 332 (4th Cir. 1997).

123. For example, the manager of the site that hosted offensive comments about Yale law students states that the goal of his site is the creation of a community where users can freely express themselves. See Martineau, *supra* note 48.

124. See *Zeran*, 129 F.3d at 333.

protection, and thus the removal of such content does not burden free speech on the Internet.<sup>125</sup> Others suggest additional laws that would penalize abusers of a notice system.<sup>126</sup>

It should be noted that *Zeran* continues to be the leading interpretation of the CDA by most courts.<sup>127</sup> Thus, until Congress addresses the perceived flaws in the statute, or the Supreme Court overrules *Zeran*, plaintiffs seeking restitution for Internet defamation must abandon the easier route of holding the ISP liable and go after the party actually posting the allegedly defamatory content.

### B. *Striking a Balance*

The courts that have developed guidelines for unmasking anonymous Internet defendants all reasoned to their respective standards by attempting to strike an appropriate balance between the First Amendment's guarantee of anonymous expression and the restrictions on defamatory speech.<sup>128</sup> Each court's assessment is considered below.

#### 1. *Dendrite's Balance*

The crux of the *Dendrite* standard is the third prong of its four-prong test: the plaintiff must be able to survive a motion to dismiss by providing sufficient evidence for each element of his cause of action on a prima facie basis.<sup>129</sup> The New Jersey appellate court had to decide whether anonymous comments on a Yahoo! message board—alleging that Dendrite made changes in its accounting to boost earnings and that Dendrite's president was secretly looking to sell the company<sup>130</sup>—were protected opinions of the John Doe poster. If so, Doe's identity should remain anonymous. If not, the statements amounted to defamation, and Doe should not be afforded the protections of anonymity.<sup>131</sup>

---

125. See, e.g., Ottenweller, *supra* note 33, at 1331.

126. See SOLOVE, *supra* note 3, at 155. Solove does not elaborate on the appropriate form of penalization or how courts would prove abusiveness. He also fails to consider cases where the speech does not rise to the level of defamation, but is nonetheless hurtful and could be construed by the individual (and the ISP) as defamation. In such cases, the notice request should be denied, but the request itself would not be abusive and subject to penalty. The ISP, therefore, would be in the precarious position of having to delete a comment or face a potential lawsuit, regardless of the ultimate determination of that suit.

127. See, e.g., Donato v. Moldow, 865 A.2d 711, 718 (N.J. Super. Ct. App. Div. 2005); Ottenweller, *supra* note 33, at 1304. *But see* Barrett v. Rosenthal, 5 Cal. Rptr. 3d 416, 429, 442 (Ct. App. 2003) (holding that ISPs, as distributors, are not immunized by the CDA).

128. Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) (“[W]e must adopt a standard that appropriately balances one person’s right to speak anonymously against another person’s right to protect his reputation.”); Dendrite Int’l, Inc. v. Doe, 775 A.2d 756, 766 (N.J. Super. Ct. App. Div. 2001); *In re* Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000).

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

130. *Id.* at 763.

131. *Id.* at 766.

On appeal, Dendrite argued that the lower court incorrectly decided its motion to compel discovery by imposing an inappropriate burden of proof when it evaluated whether Dendrite could survive a motion to dismiss.<sup>132</sup> The court found that Dendrite could not survive a motion to dismiss because it had failed to make a prima facie case against the John Doe defendant for defamation.<sup>133</sup> Specifically, the court held that Dendrite failed to show any actual harm to the corporation based on the allegedly defamatory statements.<sup>134</sup>

The appellate court agreed with Dendrite that the lower court required more evidentiary support than traditionally necessary when deciding a motion to dismiss.<sup>135</sup> It upheld the actual harm requirement, however, stating that “application of our motion-to-dismiss standard in isolation fails to provide a basis for an analysis and balancing of Dendrite’s request for disclosure in light of John Doe No. 3’s competing right of anonymity in the exercise of his right of free speech.”<sup>136</sup> Proof of actual harm, rather than simply pleading a defamation cause of action, is necessary to prevent plaintiffs from harassing, intimidating, or silencing critics on the Internet.<sup>137</sup> In this case, Dendrite could not show actual harm, and the trial court’s denial of discovery was upheld.<sup>138</sup>

Interestingly, even if Dendrite had provided sufficient proof of harm, the four-step standard adopted by the appellate court required an additional step before compelling discovery: balancing Doe’s First Amendment right against the strength of Dendrite’s prima facie case.<sup>139</sup> It is thus conceivable that a plaintiff could survive a motion to dismiss at the third step, yet still be unable to proceed because the court would not compel disclosure of Doe’s identity at the fourth step.<sup>140</sup>

## 2. Cahill’s *Balance*

The *Cahill* court faced an interesting—and arguably more important<sup>141</sup>—factual scenario than those presented in many anonymous defamation lawsuits. Whereas most reported cases involve individuals or

---

132. *Id.*

133. *Id.* at 768.

134. *Id.*

135. *Id.* at 769.

136. *Id.* at 770.

137. *Id.* at 771.

138. *Id.* at 772. Dendrite claimed that the message board posts caused a drop in its stock price and may have affected its ability to hire future employees. *Id.* Both courts felt this connection was too tenuous to prove actual harm. *Id.* Dendrite’s stock price went down in the days following some of Doe’s posts, but it also increased on days immediately following other posts. *Id.* Further, Dendrite offered no evidence to bolster its allegation that the postings actually affected its hiring practices. *Id.*

139. *Id.* at 760–61.

140. *See id.*

141. *See* Martin, *supra* note 8, at 1237–44 (discussing the importance of anonymous political speech in the Supreme Court’s First Amendment jurisprudence and the need for an alternate unmasking standard in cases involving political speech).

corporate entities seeking redress against anonymous speakers,<sup>142</sup> Patrick Cahill was a politician seeking the identity of a private citizen who criticized his duties as city councilman.<sup>143</sup> Thus, the court's ultimate determination of Cahill's right to pursue false and malicious speech had to be weighed against Doe's legitimate right to speak in political dissent.<sup>144</sup> Unmasking Doe for taking an unpopular political stance, without definitive proof of defamation, would be stripping him of his "shield from the tyranny of the majority."<sup>145</sup>

With the costs and benefits of unmasking Doe properly framed, the Delaware Supreme Court considered the appropriate standard to apply. The court rejected the lower court's adoption of the good faith standard, which called for Cahill to establish "(1) that [he] had a legitimate, good faith basis upon which to bring the underlying claim; (2) that the identifying information sought was directly and materially related to [his] claim; and (3) that the information could not be obtained from any other source."<sup>146</sup> The court reasoned that this standard did not afford sufficient protection for the speaker.<sup>147</sup> Armed with a pleading initially sufficient to meet the first two steps of the standard, defamation plaintiffs could obtain a key form of relief—the speaker's identity—even if they did not intend to pursue the action further.<sup>148</sup> Plaintiffs could then pursue remedies outside the legal system if they lost their defamation case on the merits, or pursue them immediately upon learning the speaker's identity.<sup>149</sup> If it adopted such a minimally protective standard, the court would discourage debate on important issues of public concern by taking away an anonymous poster's only protection for expressing unpopular ideas.<sup>150</sup> At the same time, public figures would be encouraged to stamp out dissent—or at least identify and address it—through the threat of litigation.<sup>151</sup>

The Delaware Supreme Court next rejected a motion to dismiss standard that it had previously applied in a libel case in which the identity of the defendants was known to the plaintiff.<sup>152</sup> On a motion to dismiss, a court's review is limited to the pleadings in the complaint, and it

---

142. See, e.g., *McMann v. Doe*, 460 F. Supp. 2d 259, 261–63 (D. Mass. 2006); *Best W. Int'l. Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at \*1 (D. Ariz. July 25, 2006); *Dendrite*, 775 A.2d at 759–64; *Reunion Indus. Inc. v. Doe 1*, 80 Pa. D. & C.4th 449, 449 (Ct. Com. Pl. 2007).

143. *Doe v. Cahill*, 884 A.2d 451, 454 (Del. 2005)

144. See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (“[P]olitical speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.”).

145. *Id.*

146. *Cahill*, 884 A.2d at 455.

147. See *id.* at 457–58.

148. *Id.* at 457.

149. *Id.* The court stresses the consequences by bluntly stating that “the plaintiff can simply seek revenge or retribution.” *Id.*

150. *Id.*

151. *Id.*

152. *Id.* at 458–59 (discussing *Ramunno v. Cawley*, 705 A.2d 1029 (Del. 1998)).

must draw all reasonable factual inferences in favor of the opposing party.<sup>153</sup> Noting this standard of review, the court observed “that even silly or trivial libel claims can easily survive a motion to dismiss where the plaintiff pleads facts that put the defendant on notice of his claim, however vague or lacking in detail these allegations may be.”<sup>154</sup> This is not problematic when the defendant’s identity is known because no constitutional harm comes from allowing a trivial claim to move forward—it will quickly be dismissed by the trial court via summary judgment.<sup>155</sup> Allowing a claim against an anonymous defendant to go forward on a well-pleaded complaint alone, however, will allow even trivial suits to strip anonymous defendants of their constitutional protections.<sup>156</sup> A suit without merit may eventually be dropped, but the plaintiff will know the identity of the alleged libeler and have the ability to retaliate.<sup>157</sup>

Relying on *Dendrite*, the Delaware Supreme Court adopted a summary judgment standard that requires notice of suit to the defendant and sufficient factual support for the claim to defeat a motion for summary judgment.<sup>158</sup> To survive a summary judgment motion, the plaintiff must submit sufficient evidence of each essential element of the defamation claim to establish a prima facie case.<sup>159</sup> Mindful of the impossibility of proving that the defendant made the allegedly defamatory comment with actual malice—an important element of a claim for public figure defamation under Delaware law—without first discovering the defendant’s identity, the court held that the plaintiff “must only plead and prove facts . . . that are within his control.”<sup>160</sup> Thus, the plaintiff does not have to produce evidence of actual malice in order to survive summary judgment.<sup>161</sup>

The court further noted that the unique characteristics of the Internet were not relevant to its balance of First Amendment rights and enforcement of defamation claims.<sup>162</sup> Thus, an anonymous Internet defendant is afforded the same protections as the author of an anonymous pamphlet,<sup>163</sup> and the plaintiff seeking the identity of the pamphleteer must also meet the summary judgment standard.<sup>164</sup> The appropriate balance is one that recognizes and protects a speaker’s right to anonymous speech, but prevents abuse of that right by mandating the revelation of a

---

153. *Id.* at 458.

154. *Id.* at 459.

155. *Id.*

156. *Id.*

157. *Id.* at 458.

158. *Id.* at 460–61; *see also* discussion *supra* Part II.D.2.

159. *Cahill*, 884 A.2d at 463.

160. *Id.* at 464.

161. *Id.*; Martin, *supra* note 8, at 1236.

162. *Cahill*, 884 A.2d at 465.

163. An anonymous political leaflet was the medium of speech at issue in *McIntyre*. *See McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 337 (1995).

164. *Cahill*, 884 A.2d at 465 (“[W]henever a defamation plaintiff seeks to unmask an anonymous defendant, we apply the summary judgment standard regardless of the chosen medium of publication.”).

speaker's identity when a plaintiff has conducted an appropriate factual investigation into the harmful speech that supports a defamation claim.

Not all courts agree with the *Cahill* balance.<sup>165</sup> In *McMann v. Doe*, a federal district court noted that a plaintiff need not show actual malice when proving his case in the face of a *Cahill* summary judgment motion.<sup>166</sup> The court considered this problematic because the Supreme Court uses actual malice to balance First Amendment protections in defamation cases involving public concern.<sup>167</sup> By eliminating proof of actual malice from its summary judgment standard, a public figure could potentially unmask dissidents who prefer to remain anonymous and thereby chill disagreeable speech.<sup>168</sup> The court does go on to say, however, that despite its misgivings about the specifics of the summary judgment test, it is reasonable for courts to apply some form of screening to a plaintiff's claim before authorizing a subpoena.<sup>169</sup>

### 3. *The Good Faith Balance*

In *In re Subpoena Duces Tecum to America Online, Inc.*, the Virginia Circuit Court considered the First Amendment rights of five anonymous speakers in relation to potentially defamatory comments about a publicly traded company made in AOL chat rooms.<sup>170</sup> It ultimately concluded that the identity of an anonymous defendant can be revealed if necessary to advance the plaintiff's claim and the claim asserts a "legitimate, good faith basis" for bringing a defamation suit.<sup>171</sup>

The court recognized the importance of the First Amendment rights at stake.<sup>172</sup> Unlike the court in *Cahill*, however, it considered the unique characteristics of the Internet when adopting its standard.<sup>173</sup> Noting that a state has a compelling interest in protecting companies incorporated within its borders, the court ruled that limited intrusion on the First Amendment rights of innocent users was significantly outweighed by the interest in protecting companies from the potentially severe consequences that "could easily flow from actionable communications" on the Internet.<sup>174</sup>

---

165. See, e.g., *McMann v. Doe*, 460 F. Supp. 2d 259, 267–68 (D. Mass. 2006).

166. *Id.* at 267.

167. *Id.*

168. *Id.*

169. *Id.* at 268.

170. 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000); see discussion *supra* Part II.D.3.

171. *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372, at \*8.

172. *Id.* at \*5–7.

173. *Compare Doe v. Cahill*, 884 A.2d 451, 465 (Del. 2005) (stating that the court did not rely on the nature of the Internet when adopting its summary judgment standard), with *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372, at \*6 (noting that the Internet "provides a virtually unlimited, inexpensive, and almost immediate means of communication" with millions of potential readers and thus could be dangerously misused).

174. *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372, at \*8 (emphasis added).

### C. Summary

This Part shows the importance of the CDA within Internet defamation jurisprudence. Its interpretation in *Zeran*, adopted by many courts, left those same courts with a difficult First Amendment challenge when plaintiffs sought remedy for allegedly defamatory speech posted by anonymous Internet defendants. The next Part proposes a solution that encourages the explicit adoption of *Zeran* and asks courts grappling with Internet defamation claims involving anonymous defendants to consider the plaintiff's position within (or without) the public eye.

## IV. RECOMMENDATION

As the above survey of Internet defamation case law illustrates, most plaintiffs bringing suit against anonymous Internet defendants are either businesses or public figures.<sup>175</sup> Thus, none of the standards that courts have developed for unmasking anonymous online speakers properly considers the privacy concerns of ordinary citizens.<sup>176</sup> By virtue of their special role in society, whether via public discourse (for public figures)<sup>177</sup> or consumer markets for goods and services (for corporate entities),<sup>178</sup> courts have had to carefully balance the First Amendment issues at stake when suits are brought by well-known or established plaintiffs. Yet, this balance is hardly necessary when the plaintiff is a private figure whose interest in preventing online defamation is not to chill dissenting speech but to protect a reputation that was never meant for the public spotlight.<sup>179</sup>

Much of the current literature addressing Internet defamation also focuses on corporate plaintiffs and political speech.<sup>180</sup> Understandably,

---

175. See discussion and cases cited *supra* Parts II–III.

176. See Victor Siber & Lisa K. Marino, *Unmasking Online Defendants: Addressing the Anonymous Posting of Rumors While Preserving the First Amendment*, N.Y.L.J., Apr. 9, 2007, at S4.

177. See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 342 (1974) (defining public figures as those whose achievements have brought them some level of notoriety, or those who, with vigor and success, seek public attention).

178. See Lidsky, *supra* note 51, at 872 (describing the notion that corporate defamation plaintiffs bring suit not for monetary damages but to suppress legitimate criticism).

179. Compare *Best W. Int'l, Inc. v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, at \*3 (D. Ariz. July 25, 2006) (describing the nonprofit member corporation seeking the identity of anonymous Internet posters), and *Doe v. Cahill*, 884 A.2d 451, 454 (Del. 2005) (describing alleged defamatory remarks about a city councilman), with Anna Badkhen, *Web Can Ruin Reputation with Stroke of a Key*, S.F. CHRON., May 6, 2007, at A1 (detailing how online smear campaigns “can wreak havoc” in the lives of the victims).

180. See, e.g., Lidsky, *supra* note 51, at 892; *Trende*, *supra* note 39, at 607; *Martin*, *supra* note 8, at 1218. But see Caitlin Hall, Note, *A Regulatory Proposal for Digital Defamation: Conditioning § 230 Safe Harbor on the Provision of a Site “Rating,”* 2008 STAN. TECH. L. REV. N1, <http://stlr.stanford.edu/pdf/hall-digital-defamation.pdf>. Hall proposes “that the distinction between public and private figures be abolished” in Internet defamation cases. *Id.* ¶ 36. Her proposal stems from the notion that Internet access is much easier for plaintiffs, who can counteract negative comments by posting rebuttals online and reaching relevant audiences. *Id.* ¶ 14. Traditional defamation plaintiffs do not have this opportunity as media access is generally limited to public figures. *Id.* Although it is true that almost

these cases implicate one of the First Amendment's essential protections—freedom to express unpopular opinions without tyrannical reprisal from the majority—and thus invoke passionate intellectual debate. Although it is easy to appreciate and agree with many of the points made in this ongoing debate, any solution to the problem of anonymous Internet defamation that ignores or fails to properly consider the interests of private citizens is ultimately unworkable and will encourage destructive communication.<sup>181</sup> This Part proposes a tiered system of unmasking standards that asks courts to first categorize the plaintiff as public, corporate, or private. Successful implementation of this plan, however, will require revisiting the CDA.

A. *Zeran Must Be Codified in the Communications Decency Act*

A real solution to the problem of anonymous defamation on the Internet must first address the CDA and its interpretation by courts as immunizing ISPs from distributor liability in defamation cases. The Internet has grown in popularity and usage since the passage of the CDA.<sup>182</sup> This growth is partially attributable to the immunities provided by both the CDA and the *Zeran* line of cases interpreting it. Free of litigation fears, ISPs have been able to provide countless forums for free expression.<sup>183</sup> These forums continue to allow users the ability to communicate across local, national, and international borders.<sup>184</sup> A policy that encourages communication decency but does not mandate it—as the *Zeran* interpretation of the CDA holds—is preferable to one that forces providers of Internet chat rooms and message boards into positions of decision making better suited for juries or the bench. The alternative threatens to scale back the growth and effectiveness of Internet communication.

Congress should amend the CDA as currently written and explicitly incorporate the *Zeran* decision into its text. Though the CDA clearly immunizes an ISP from liability when actively editing defamatory content, the language is less clear regarding immunity when no action is taken. This ambiguity allows courts to move away from the *Zeran* line of reasoning and adopt interpretations less favorable to online speech.<sup>185</sup> By amending the CDA, Congress will send a clear message to courts considering this issue that it intends to immunize all ISPs from publisher and distributor liability, regardless of the editorial control exercised.

---

anyone who wants to publish online can do so, *id.*, it is unlikely that a private defamation victim's blog post rebutting false statements will have the same effect as a media retraction, or reach the same audience that read the defamatory comments.

181. Many Web sites that encourage people to post gossip and rumors about others thrive under the CDA's broad immunity. See SOLOVE, *supra* note 3, at 159.

182. See Trende, *supra* note 39, at 610.

183. See SOLOVE, *supra* note 3, at 159, 204.

184. See Ciarlone & Wiechmann, *supra* note 37, at 61.

185. See, e.g., Barrett v. Rosenthal, 5 Cal. Rptr. 3d 416, 432 (Ct. App. 2003).

Further, an explicit CDA amendment puts plaintiffs on notice that alleged defamation must be traced to its source, thereby reducing costly and unnecessary litigation.<sup>186</sup> A party cannot attempt to “win the lottery” by suing an ISP for alleged defamatory content and hoping for a quick and easy settlement. By making the process more difficult for plaintiffs, Congress will ensure that only egregious and genuine claims proceed, thus implicating the potential denial of important First Amendment protections only when completely necessary.

### *B. Holding the Actual Speaker Accountable*

Immunizing ISPs from defamation liability requires plaintiffs seeking redress to bring suit against the poster of defamatory content. Holding tortfeasors accountable for their actions is clearly preferable to lawsuits aimed at ISPs, which would be unlikely to end a pattern of defamation. Anonymous posters would find their chosen forum for posting closed if an ISP were held liable, but a plethora of sites would still be available to continue an assault on an individual’s reputation. Thus, the most effective way to end defamation on the Internet is to hold the individual making the comments accountable.

As discussed above, anonymity on the Internet makes accountability problematic. The current system, though helpful in cases involving defamatory speech against public figures and corporate entities, undervalues the privacy concerns of everyday citizens. Thus, no single unmasking standard can adequately address the interests of the various potential parties in Internet defamation cases. Instead, courts must categorize the plaintiff seeking the identity of anonymous users and apply an appropriate standard based on its categorization.

#### *1. Who Is the Victim?*

When faced with a request to compel disclosure of an anonymous Internet defendant, courts should first consider whether the alleged victim of defamation is a public figure, a business association, or a private citizen. To make this determination, courts cannot rely on the complaint or pleadings alone. To do so would invite gaming of the judicial system at the pleadings stage, as public figures could artfully draft a pleading that categorized the public figure as a private citizen. Instead, courts must carefully consider the content of the defamatory statements in question and the context in which they were delivered. Surprisingly, no court developing an unmasking standard has taken the content of the ac-

---

186. See SOLOVE, *supra* note 3, at 159 (noting the potential time and costs of litigation).

tionable speech into consideration.<sup>187</sup> By doing so, courts can more accurately assess the nature of the complaint and apply the proper standard.

2. *The Cahill Summary Judgment Standard Should Be Applied in Cases Involving Public Figures and Business Entities*

The *Cahill* standard imposes a significant burden on the plaintiff seeking an anonymous poster's identity.<sup>188</sup> Plaintiffs must produce sufficient evidence of each essential element of a defamation claim such that they can survive a motion for summary judgment.<sup>189</sup> Thus, a plaintiff cannot simply plead harm; he must show harm to reputation via substantial evidence.<sup>190</sup> If a plaintiff cannot meet this burden, the complaint must be dismissed and the anonymous user's identity cannot be revealed.

Requiring public figures to meet the summary judgment standard makes sense in light of Supreme Court jurisprudence regarding defamation claims involving those in the public eye. As the Court noted in *Gertz* regarding the standard it set in *New York Times v. Sullivan*, a high burden for the plaintiff is "an extremely powerful antidote to the inducement" of self-censorship.<sup>191</sup> Critics of public figures, particularly politicians, should not be dissuaded from making dissenting remarks by the threat of defamation litigation. Nor should those same critics, fearful of public scorn for voicing an unpopular opinion and thus choosing to speak anonymously, feel pressured to remain quiet by the specter of a subpoena demanding their identification.

Not everyone believes the summary judgment standard is appropriate in cases of political speech.<sup>192</sup> Removing actual malice from the equation seems to fly in the face of Supreme Court precedent.<sup>193</sup> An additional balancing step, however, is not necessary. Public figures must still produce sufficient evidence to show that their reputation was significantly damaged by the allegedly defamatory comments. In an age when much of what is written on the Internet is viewed with at least some mild skepticism, particularly in unmoderated forums where anonymous posters have free reign,<sup>194</sup> a showing of actual harm is enough to legitimize defamation claims. Even if they are unmasked, defendants could win at trial if discovery fails to produce actual malice evidence. This is a risk anonymous Internet posters face, and one that will curb only truly defamatory comments. If *Cahill* is applied correctly, courts should not un-

---

187. Martin, *supra* note 8, at 1237. *But see* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237 (Ct. App. 2008).

188. See discussion *supra* Parts II.D.2, III.B.2.

189. Doe v. Cahill, 884 A.2d 451, 464 (Del. 2005).

190. *Id.*

191. Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974).

192. Martin, *supra* note 8, at 1242-43.

193. McMann v. Doe, 460 F. Supp. 2d 259, 267 (D. Mass. 2006); Martin, *supra* note 8, at 1242-43.

194. See *Cahill*, 884 A.2d at 465.

mask anonymous defendants for criticisms or commentary that do not rise to the level of defamation.

The summary judgment standard is also appropriate for corporate entities looking to unmask anonymous Internet critics. Evidence suggests that corporations often bring defamation suits to silence critical speech, regardless of whether it is defamation.<sup>195</sup> Thus, before allowing a corporate plaintiff to unmask anonymous critics, courts should require it to produce sufficient evidence to show that it was harmed as a direct result of the statements in question. As with public figures, the *Cahill* standard appropriately balances First Amendment rights while still allowing legitimate defamation claims to move forward.

### 3. *The Good Faith Standard Should Be Adopted with a Notice Requirement in Cases Involving Private Citizens*

*Gertz* established a clear distinction between private and public figures in the realm of defamation.<sup>196</sup> As such, the Supreme Court concluded that the actual malice standard, though appropriate for public figures, did not adequately address the vulnerabilities of private individuals.<sup>197</sup> Stating that defamation law “is rooted in our experience that the truth rarely catches up with a lie,”<sup>198</sup> the Court noted that self-help remedies such as media retractions might aide public figures in combating falsehoods, but these remedies are not as easily accessible to private individuals.<sup>199</sup> Additionally, by virtue of their role in the spotlight, public figures run the risk of close public scrutiny,<sup>200</sup> and thus the media may act on the assumption that public figures voluntarily exposed themselves to the possibility of defamation.<sup>201</sup> This same assumption cannot be justified for private individuals, who have not exposed themselves to the dangers of defamation that public scrutiny entails and thus have a more urgent need for redress via the judicial system.<sup>202</sup> The Court

---

195. See, e.g., *DiMeo v. Max*, 433 F. Supp. 2d 523 (E.D. Pa. 2006); see also *Lidsky*, *supra* note 51, at 876–83 (discussing reasons corporations sue John Doe defendants and noting that silencing anonymous posters might be one of the chief motivations for such suits); *Trende*, *supra* note 39, at 629–46 (defining SLAPPs (Strategic Lawsuits Against Public Participation), how they are used to silence critics, and why federal anti-SLAPP legislation may be appropriate).

196. *Gertz*, 418 U.S. at 344.

197. *Id.*

198. *Id.* at 344 n.9.

199. *Id.* at 344.

200. *Id.*

201. *Id.* at 345 (“Even if the foregoing generalities do not obtain in every instance, the communications media are entitled to act on the assumption that public officials and public figures have voluntarily exposed themselves to increased risk of injury from defamatory falsehood concerning them.”).

202. *Id.* A private individual has not accepted public office or assumed a role in the public spotlight. *Id.* Thus, private citizens have “relinquished no part of [their] interest in the protection of [their] own good name, and consequently [they have] a more compelling call on the courts for redress of injury inflicted by defamatory falsehood.” *Id.*

concluded that states should have “substantial latitude” in enforcement efforts involving defamation of a private individual.<sup>203</sup>

Based on the Court’s conclusion, it is not a stretch to extend this latitude to Internet defamation and anonymous speech. Search engines like Google can memorialize horrendous and false comments about private individuals for years after their initial publication.<sup>204</sup> It is easier to reserve a certain level of skepticism for ugly comments regarding public figures, who can counteract such comments by virtue of their command of the public spotlight.<sup>205</sup> Google searches for a public figure will generally yield positive as well as negative comments. Unfortunately for a private individual, merely one searchable comment about him might appear.<sup>206</sup> If it is negative, a summary judgment standard poses an exceedingly difficult obstacle to redressing the harm to the individual’s reputation.

Once a court has concluded that a plaintiff is a legitimate private individual, it should carefully consider the plaintiff’s complaint and the nature of the comments at issue. If the court finds that the plaintiff has a legitimate, good faith basis for the complaint and the John Doe speaker has been provided sufficient notice,<sup>207</sup> Doe’s identity should be revealed and the plaintiff should have an opportunity to conduct discovery.

Unquestionably, this standard has the potential to curb some anonymous speech, even if it does not rise to the level of defamation.<sup>208</sup> It is hard to justify, however, protecting an anonymous speaker’s identity when harmful—though not defamatory—speech is at issue. Words can have consequences, whether spoken freely or behind the cloak of an Internet username.<sup>209</sup> Individuals willing to speak negatively about friends

---

203. *Id.* at 345–46.

204. See Anthony Ciolli, *Defamatory Internet Speech: A Defense of the Status Quo*, 25 QUINNIPIAC L. REV. 853, 860–61 (2007).

205. The Supreme Court notes that the first remedy for any defamation victim is self-help. See *Gertz*, 418 U.S. at 344. This involves the use of any available opportunity “to contradict the lie or correct the error and thereby minimize its adverse impact on reputation.” *Id.* Public figures generally have “significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements.” *Id.*

206. Ciolli, *supra* note 204, at 860–61 (noting differences in Google searches for public figures).

207. There is also a wide range of notice options available for courts to consider. See Gleicher, *supra* note 91, at 347–49 (describing direct notice, notice via the same method used to express the actionable speech, and publication notice). For purposes of the relaxed good faith standard, the notice requirement articulated in *Cahill* is sufficient: “[T]he plaintiff must post a message notifying the anonymous defendant of the plaintiff’s discovery request on the same message board where the allegedly defamatory statement was originally posted.” *Doe v. Cahill*, 884 A.2d 451, 461 (Del. 2005).

208. If individuals know that their speech is not truly anonymous and their real name could be linked to Internet posts, they will be more reluctant to post objectionable content in the first place. For instance, one of the contributors to the message boards used to facilitate negative comments against the Yale students had his law firm job offer revoked when his real name was linked with the Web site. See Posting of Amir Efrati to the Wall Street Journal Law Blog, *Law Firm Rescinds Offer to Ex-AutoAdmit Executive*, <http://blogs.wsj.com/law/2007/05/03/law-firm-rescinds-offer-to-ex-autoadmit-director/> (May 3, 2007, 11:02 EST).

209. SOLOVE, *supra* note 3, at 189 (noting that gossip and false rumors can “wreak havoc on reputations”).

or strangers, even in jest, should be equally willing to own their comments when they are objected to. This means accepting the stigma and embarrassment of being associated with gratuitous language.<sup>210</sup> Further, though this standard is much easier to meet than the *Cahill* standard, a notice requirement provides some additional protection to the defendant, who can then step forward anonymously through a lawyer and challenge the unmasking decision.<sup>211</sup>

It should also be noted that neither legitimate criticism nor dissent is included in this category of harmful speech. Objectionable language targeting specific private citizens, however, is rarely legitimate criticism.<sup>212</sup> By examining the context of the litigated comments, courts should be able to tell the difference. Furthermore, courts that unmask an anonymous defendant for such speech are not stripping the defendant of all First Amendment rights. Rather, they are merely exposing the identity of the speaker, who could ultimately prevail in the underlying lawsuit on First Amendment grounds.<sup>213</sup> Perhaps this exposure will stop some anonymous speech. Promoting decency and civilized discourse, however, is not necessarily a bad thing.<sup>214</sup>

## V. CONCLUSION

Freedom to speak, both on the record and anonymously, is one of our nation's most cherished rights. This right, however, is not absolute. Ugly, demonstrably false statements have no place in public discourse. The Internet, though still young relative to other mediums of communication, is no different from traditional forms of communication. Though it offers easier access and more opportunity to comment anonymously, users cannot abuse this freedom by committing defamation and hiding behind the First Amendment. Congress and the courts have admirably

---

210. See Efrati, *supra* note 208. The student, when first questioned by his firm about his association with the Web site, admitted to learning a valuable lesson from the incident, including "the importance of good judgment and proceeding with caution." *Id.*; see also David Margolick, *Slimed Online*, CONDÉ NAST PORTFOLIO, Mar. 2009, at 80, available at <http://www.portfolio.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying> (discussing litigation filed by the Yale law students and subsequent settlements of some anonymous defendants who did not want their identities publicized).

211. See Martin, *supra* note 8, at 1227.

212. See, e.g., *Doe I v. Individuals*, 561 F. Supp. 2d 249, 250–52 (D. Conn. 2008). The comments at issue could not be objectively viewed as legitimate criticism, but are merely gratuitous personal attacks.

213. See *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 118 (1991) ("[T]he fact that society may find speech offensive is not a sufficient reason for suppressing it. Indeed, if it is the speaker's opinion that gives offense, that consequence is a reason for according it constitutional protection." (citation omitted)).

214. See SOLOVE, *supra* note 3, at 189–205 (examining the ways reputations can be tarnished in the future and considering whether our reputations can be protected in the age of the Internet); see also Margolick, *supra* note 210 (noting the change in some of the rhetoric on AutoAdmit.com, the message board on which offensive comments about the Yale students were posted, since the students brought suit and sought to expose users' real names).

balanced the First Amendment and the rights of public figures regarding anonymous online defamation. But in the search for a proper solution, they have failed to address the concerns of everyday, private citizens. The alternate standard proposed here conforms to the Supreme Court's belief that privacy deserves more protection when the individual involved is not, nor has ever been, under the glare of the public spotlight.

