Loyola of Los Angeles Law Review

Volume 44
Number 2 *Winter 2011 - Symposium: Rebooting California: Initiatives, Conventions & Government Reform*

Article 13

1-1-2011

I Am He as You Are He as You Are Me: Being Able to Be Yourself, Protecting the Integrity of Identity Online

Wesley Burrell
Loyola Law School Los Angeles, wesley.burrell@lls.edu

I AM HE AS YOU ARE HE AS YOU ARE ME: BEING ABLE TO BE YOURSELF, PROTECTING THE INTEGRITY OF IDENTITY ONLINE

*Wesley Burrell**

Arguing for an individual's right to integrity of identity online, this Note advocates rolling back broad immunity for Internet service providers (ISPs) under § 230 of the Communications Decency Act as interpreted in Zeran v. America Online, Inc. *Exploring the theoretical foundation and modern application of the right of publicity, this Note reasons that traditional right-to-privacy notions support a right to control one's identity online, recognition of which is necessary in the Web 2.0 era. Because ISPs are the greatest beneficiaries of Web 2.0's identity-driven structure and are in the best position to aid users in regulating their online identities, ISPs must be made to bear a greater portion of the burden to protect users and maintain an environment of safe interaction online. This Note concludes with a proposal for accomplishing this.*

* J.D. Candidate, May 2011, Loyola Law School Los Angeles. I would like to extend a very special thanks to my wife Talene and my Mom and Dad. I would also like to thank Professor John Nockleby for his time and guidance, as well as my family and loved ones for their support and encouragement.

TABLE OF CONTENTS

I. INTRODUCTION

Over the last decade, Americans have seen an unprecedented increase in integration between the online and offline worlds. Internet usage is increasingly ubiquitous,[1] its nature more and more interactive and participatory.[2] The twentieth-century Internet was conceived primarily as an information-providing platform with users on the receiving end.[3] Online activity was predominately fit to that conception—akin to viewing television or reading a book. Today, by contrast, users log more online hours using interactive social media than they spend passively receiving prepackaged information and entertainment.[4] They are communicating, self-expressing, and contributing to the development of culture and community, and they are doing so with more ease and frequency than they ever did before.[5] Beneficially, this allows them to engage with society, enrich themselves, and impact others like never before.[6] But there is a dark side as well. This shift in Internet usage brings an attendant shift in the relationship between the virtual world online and the real world offline, which increases the risk and danger associated with Internet use. Current law does not provide adequate protection against this dark side.

To illustrate the dark side of the interconnected online and offline worlds, consider the facts of *Barnes v. Yahoo!, Inc.*[7] In early 2005, the unsuspecting Cecilia Barnes began to receive phone calls and emails from strangers soliciting sex.[8] They called her at work and even solicited her in person.[9] They assumed that she wanted the

1. *See United States of America Internet Usage and Broadband Usage Report*, INTERNET WORLD STATS, http://www.internetworldstats.com/am/us.htm (last visited Jan. 18, 2010) (noting that in 2009, 74.1 percent of the U.S. population used the Internet); Christina Warren, *Average Internet User Now Spends 68 Hours Per Month Online*, MASHABLE (Oct. 14, 2009), http://mashable.com/2009/10/14/net-usage-nielsen.

2. Enid Burns, *More Time Spent Online Communicating Than Getting Entertained*, CLICKZ (Mar. 3, 2009), http://www.clickz.com/3632986.

3. Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY (Sept. 30, 2005), http://www.oreillynet.com/lpt/a/6228.

4. Enid Burns, *Study: Social Media's Hot, Entertainment's Not*, CLICKZ (Dec. 12, 2008), http://www.clickz.com/3632063.

5. Burns, *supra* note 2.

6. *See, e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105 (9th Cir. 2009); *infra* note 27.

7. 570 F.3d 1096 (9th Cir. 2009).

8. *Id.* at 1098.

9. *Id.*

attention, that she had requested it. Finally, Barnes discovered the cause: someone had posted a personal ad soliciting casual sex on Yahoo! Personals ("Yahoo") with her name and contact information.[10] The ad had been posted without her knowledge or permission and was viewable by Internet users all over the world.[11] It displayed nude photos of her taken without her knowledge and listed personal information including her email, work address, and phone number.[12] The anonymous poster had also conducted online discussions in Yahoo chat rooms.[13] Posing as Barnes, the poster propositioned men and directed them to the fake personal ad for further information and interaction.[14] Using Barnes's fraudulently misappropriated identity, the poster actively solicited strangers to unwittingly harass Barnes.[15]

Upon discovery of the fraudulent profile, and having no other recourse against the anonymous poster, Barnes followed Yahoo's official policy for requesting removal of web content.[16] She mailed Yahoo a copy of her photo ID, a signed statement denying her involvement with the profile, and a request for Yahoo to remove the profile.[17] Nevertheless, the profile remained.[18] For months, Barnes mailed requests for removal with no results.[19] Yahoo did not respond until a local news program prepared to air a report on the story.[20] Yahoo's Director of Communications called Barnes personally and asked her to fax copies of all previous requests for removal.[21] The director promised to "take care of it" personally.[22] Barnes faxed the correspondence and, relying on the director's reassurance, took no further action.[23] Yet, two months passed, the profile remained active,

10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.* at 1098–99.
21. *Id.* at 1099.
22. *Id.*
23. *Id.*

and harassment continued.[24] Not until Barnes sued Yahoo did the profile disappear.[25]

Sadly, Barnes's predicament is not an anomaly.[26] This form of harassment is common in today's online culture.[27] Even children have been its victims.[28] But harassment and the danger of assault are not the only consequences of identity misappropriation. Whenever online impersonators post unauthorized images, unapproved personal information, or other fraudulent source-identifying content, such postings are potentially detrimental to a victim's online persona and can have dangerous and destructive effects offline as well.[29] Additionally, because many Internet applications now track an individual's online identity to increase functionality and precision,[30] dilution resulting from misappropriation can impair the functionality of user-driven applications and, in some cases, drive victims offline entirely.[31]

24. *Id.*

25. *Id.*

26. Eric Goldman, *47 USC 230 Trifecta of Cases*—Friendfinder, e360insight, iBrattleboro, TECH. & MARKETING L. BLOG (Apr. 28, 2008, 10:27 AM), http://blog.ericgoldman.org/archives/2008/04/47_usc_230_trifecta.htm ("Fake dating profiles have been the source of a fair amount of 230 litigation . . . ."); *see, e.g.*, Fighter Team, *Internet Harassment & Revenge Is a Crime*, EXPOSING ONLINE PREDATORS & CYBERPATHS (Aug. 7, 2010, 7:21 PM), http://cyberpaths.blogspot.com/2009/02/internet-harassment-revenge-is-crime.html (recounting the story of "Pilar Stofega, 34, [who] spent hours crafting fake profiles about her ex-boyfriend's wife and posting them online").

27. *See, e.g.*, Landry-Bell v. Various, Inc., No. Civ.A. 05-1526, 2005 WL 3640448, at *1 (W.D. La. 2005) (representing a case with facts nearly identical to those of *Barnes*); *Telling the Difference Between Flaming, Cyber-Bullying and Harassment and Cyberstalking (A Guide for Law Enforcement)*, STOP CYBERBULLYING, http://www.stopcyberbullying.org/lawenforcement/telling_the_difference.html (last visited Oct. 22, 2009) (listing as examples of cyber-bullying: "[r]egistering [someone else's] name and setting up a bash Web site or profile," "[m]asquerading as [someone else] for any purpose," and "[p]osting [someone's] . . . cell phone number online to encourage abuse and increase . . . charges").

28. Christina Chatalian, *Cyber Stalker Terrorizing Family*, CNYCENTRAL.COM (Feb. 15, 2008, 7:10 PM), http://www.cnycentral.com/news/story.aspx?id=96646 (describing a 2008 case where an anonymous stranger stole pictures of a woman's twelve-year-old daughter and posted them on the Internet in a fake profile that included her home address, personal information, and a professed desire to be raped by a stranger).

29. *See, e.g.*, Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 78–80 (2009) (citing cases where women's names and images were purposefully posted to white supremacist watch sites to affect their employment opportunities).

30. Christopher Mims, *Who Controls Identity on the Web?*, TECH. REV. (May 13, 2010), http://www.technologyreview.com/computing/25298/?a=f.

31. Citron, *supra* note 29, at 101.

While victims have sought to protect themselves against such violations by suing for conventional right-to-privacy torts,[32] the strong protection of anonymous web posters and broad immunity for Internet service providers (ISPs) and website operators, or online service providers (OSPs), render traditional torts toothless. The lack of effective recourse against such misappropriation chills public discourse online, interferes with user-driven network advancements, and generally disrupts the increasing use of identity-syncing technologies. As a result, identity misappropriation hinders the utility and development of the Internet as a whole. It thus runs contrary to the societal good of a robust Internet that Congress expressly intends to promote.[33] Nonetheless, current law fails to adequately protect Internet users and the integrity of their online identities.

Management of Internet content is the central concern in protecting the integrity of identity online.[34] The principal law governing Internet content management is § 230 of the Communications Decency Act (CDA). Section 230 grants ISPs immunity from publisher liability for content posted by third parties, stating that "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[35] The 1997 Fourth Circuit ruling in *Zeran v. America Online, Inc.*[36] construed § 230 immunity broadly.[37] The court there read § 230's grant of immunity to encompass not only publisher liability but also notice-based distributor liability.[38] Subsequent to *Zeran*, courts have generally adopted its reasoning and applied broad immunity to both ISPs and OSPs, shielding them from nearly all liability with respect

32. *See, e.g.*, Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 291 (D.N.H. 2008) (discussing plaintiff bringing various privacy tort claims, including invasion of privacy, defamation, negligence, intentional infliction of emotional distress, and violation of right to publicity).

33. 47 U.S.C. § 230(b)(1)–(2) (2006) ("It is the policy of the United States—(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services . . . .").

34. *See id.* § 230(b).

35. *Id.* § 230(c)(1).

36. 129 F.3d 327 (4th Cir. 1997).

37. *Id.* at 332–33.

38. *Id.* at 332 ("The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law.").

to content posted by third parties.[39] Such broad immunity leaves victims of identity infringement, such as Barnes, with no means to compel ISPs or OSPs to remove tortious or misappropriating content from their websites.

Furthermore, ISPs have little incentive to collect and maintain the Internet protocol (IP) addresses[40] of anonymous posters who may have posted infringing material on their websites.[41] Those ISPs that do maintain this data routinely clear their records, some as frequently as every sixty days.[42] Thus, victims have a very limited time during which to compel an ISP to disclose a third-party poster's identity, and they often fail in their efforts to do so.[43] The resulting system grants ISPs all but total immunity, grants anonymous harassers a sort of de facto immunity, and leaves victims to absorb the expenses and injuries that result from the infringing posts. To deter identity infringement and uphold the societal interest in a robust Internet, users must be granted legal leverage against ISPs to compel the removal of infringing posts and to deter third-party posters. This leverage would be both consistent with Congress's aim and intent that underlie the CDA and is consistent with the plain language of § 230, which does not address notice-based distributor liability.

The current legal scheme is premised on an understanding of the Internet that is nearly fifteen years out of date. When the *Zeran* court interpreted *publisher* liability to include notice-based distributor liability, it did so with a different Internet in mind. Unlike 1997's Internet, today's Internet is ubiquitous and integral to contemporary

39. *See, e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105–06 (9th Cir. 2009); Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288 (D.N.H. 2008).

40. "An IP address is a unique, electronic number which specifically identifies a device (often a computer) connected to the Internet." Tara E. Lynch, *Good Samaritan or Defamation Defender? Amending the Communications Decency Act to Correct the Misnomer of § 230 . . . Without Expanding ISP Liability*, 19 SYRACUSE SCI. & TECH. L. REP. 1, 18 (2008) (citation omitted), *available at* http://sstlr.syr.edu/wp-content/uploads/lynch-final-version.pdf.

41. Citron, *supra* note 29, at 118 (noting that broad immunity "eliminate[s] incentives for better behavior" as operators have no reason to "collect and retain the identities of posters").

42. *Where Is Your Data?*, ISP DATA RETENTION (July 7, 2008), http://whereismydata.wordpress.com/tag/isp-data-retention; *see also, e.g.*, Lynch, *supra* note 40, at 15 (discussing how the plaintiff in *Zeran* could not identify the John Doe who defamed him because AOL failed to maintain adequate user records).

43. *See* Plaintiffs' Memorandum of Law in Support of Motion for Expedited Discovery, Doe I v. Ciolli, 611 F. Supp. 2d 216 (D. Conn. Jan. 24, 2008) (No. 3:07-cv-909(CFD)) [hereinafter Plaintiffs' Memorandum], *available at* http://s.wsj.net/public/resources/documents/WSJ_DEF_MemoofLawreM_012408.pdf.

culture.[44] The *Zeran* court could not have anticipated the participatory nature of twenty-first century cyberspace and the degree to which identity is an integral component of its functionality. Today, "network effects from user contributions are the key," and a multi-user, collaborative approach to content creation and development is the model for success on the Internet and with other networking technologies—a paradigm that has been dubbed "Web 2.0."[45] It is not merely a matter of the more the merrier. In today's online environment, interactivity and the participation of myriad diverse users are central to the Internet's success.[46] User security and autonomy of identity are therefore of fundamental importance. The law must protect users or it will impede the Internet's continuing development by failing to facilitate plentiful participation.[47]

This Note proposes solutions to bring online protection up to date while maintaining an appropriate degree of ISP immunity. This proposal requires minimal legislation. It argues that the reality and trajectory of current technologies and the structure and nature of the Web 2.0 Internet compel a reconsideration of the dominant interpretation of § 230 of the CDA with regard to the original congressional intent. Because of the unique character of online identity and its impact on real-world persona, courts must recognize and protect the right to integrity of identity online in the same way that they have protected the rights to intellectual property online. Finally, this Note argues that Congress must enact uniform standards to ensure accountability for third-party posting online. Without such protections, individuals will remain subject to threat and continue to bear the bulk risk for participation in the Internet's virtual world, causing online culture and its marketplace of ideas to suffer.

44. Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1176 (9th Cir. 2008) ("The ubiquity of the Internet is undisputed.").

45. O'Reilly, *supra* note 3 (emphasis omitted).

46. *See id.*

47. *See* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 154 (Ct. App. 2004) ("The view of most scholars who have addressed the issue is that *Zeran*'s analysis of § 230 is flawed, in that the court ascribed to Congress an intent to create a far broader immunity than that body actually had in mind or is necessary to achieve its purposes. We share that view." (citation omitted)), *rev'd*, 146 P.3d 510 (Cal. 2006); *see also* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 293–94, 296–97 (D.N.H. 2008) (holding operators of adult web communities could not be held liable for damage caused by online profile even though plaintiff suffered "emotional distress, including anxiety over the lingering effect the false profile").

Part II will give a statement of the existing law addressing (A) privacy and publicity rights for individuals online; (B) ISP liability for third-party content; and (C) subpoena laws governing protection of anonymity and the disclosure of a third party's identity. Part III addresses the existing law's inadequacies and its failure to protect user identity online. It then discusses (A) the impact on the law discussed in Part II as it applies after the development of the Internet from the "Walled Garden" web to Web 2.0; (B) anonymity under the current law and the problems and benefits of anonymous speech when it comes to online harassment; and (C) the specific effect of existing law on victims of online harassment. In Part IV, this Note proposes changes to the existing law that will better enable individuals to protect their identities both online and, by extension, offline. Specifically, this part (A) argues from theory and common law for the development of an online right to integrity of identity; (B) proposes opening distributor liability to ISPs as an exception to § 230 immunity in the particular case of a violation of an individual's right to integrity of identity; (C) proposes a notice and takedown "safe harbor" policy for the integrity of identity exception to § 230 immunity; (D) discusses safeguards to protect speech and limit abuse of the notice and takedown policy; (E) argues for limits to online anonymity, proposes the application of a uniform subpoena policy for cases of violations of the right to integrity of identity, and discusses the privacy and free speech concerns that may stem from such limits to anonymity. In Part V, this Note discusses the judicial and legislative steps necessary to implement the proposed policies. Part VI concludes.

II. STATEMENT OF EXISTING LAW

A. Privacy and Publicity Rights Online

1. The Right of Publicity

The right of publicity is the only right to identity that courts have recognized as an exception to § 230 immunity.[48] Some courts have held that the right of publicity is an intellectual property right[49]

48. *Friendfinder*, 540 F. Supp. 2d at 301. However, not all courts recognize this exception. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123–25 (9th Cir. 2003) (holding that right of publicity claims are barred by § 230).

49. *See Carafano*, 339 F.3d at 1123–25; *see also, e.g.*, *Friendfinder*, 540 F. Supp. 2d 288,

that fits within the intellectual property exception to § 230.[50] The Restatement (Second) of Torts defines the right of publicity as an "[a]ppropriation of one's name or likeness to another's advantage."[51] The general prima facie case has three elements: (1) the defendant used the plaintiff's name, portrait, or picture; (2) for purposes of trade or advertising; (3) without written consent.[52] Its scope varies by state, but "most states now protect name, voice, signature, photograph, and likeness, almost all facets of [an individual], including persona."[53]

In *Doe v. Friendfinder Network, Inc.*,[54] the court held that a right of publicity claim is an exception to § 230 immunity.[55] There, a woman discovered a profile on a sex site identifying her by name and listing other accurate biographical information.[56] It included a nude photo with enough resemblance to her that she could be "reasonably identified."[57] She sued the ISPs Friendfinder Network, Inc. and Various, Inc. on multiple tort causes of action.[58] Citing § 230, the New Hampshire district judge dismissed all but the right of publicity claim.[59] He held that "the right of publicity is a widely recognized intellectual property right" and that it is subject to the exception for intellectual property claims.[60]

302 ("[T]he right of publicity is a widely recognized intellectual property right." (quoting Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1322 (11th Cir. 2006)); *cf. Almeida*, 456 F.3d at 1323 n.4 (declining to decide whether § 230(e)(2) immunizes ISPs from right of publicity claims but noting "the right of publicity does not fit neatly into the category of tort-based lawsuits from which Congress sought to immunize interactive service providers").

50. 47 U.S.C. § 230(e)(2) (2006) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.").

51. RESTATEMENT (SECOND) OF TORTS § 652C (1977); *see also* Eric J. Goodman, *A National Identity Crisis: The Need for a Federal Right of Publicity Statute*, 9 DEPAUL-LCA J. ART & ENT. L. 227, 232 (1999) (noting that the right of publicity is recognized directly in the common law of sixteen states with corollaries in the right to privacy or unfair competition in most others).

52. Cohen v. Herbal Concepts, Inc., 472 N.E.2d 307, 308 (N.Y. 1984).

53. Oren J. Warshavsky, *The Expanding Right of Publicity*, METROPOLITAN CORP. COUNS., Feb. 2006, at 32, *available at* http://www.metrocorpcounsel.com/current.php?artType=view&artMonth=September&artYear=2008&EntryNo=4209.

54. 540 F. Supp. 2d 288 (D.N.H. 2008).

55. *Friendfinder*, 540 F. Supp. 2d at 291.

56. *Id.* at 292.

57. *Id.* (noting that despite the resemblance, plaintiff claimed photo was not of her).

58. *Id.* at 291.

59. *Id.*

60. *Id.* at 302 (internal quotation marks omitted).

Prior to and contrary to this 2008 ruling, the Ninth Circuit had held in *Perfect 10, Inc. v. CCBill LLC*[61] that "[a]s a practical matter, inclusion of rights protected by state law within the 'intellectual property' exemption would fatally undermine the broad grant of immunity provided by the CDA."[62] As a result, the Ninth Circuit ruled that the right of publicity, trade defamation, unfair competition, and dilution, among other state intellectual property rights, were not exempted by § 230(e)(2).[63] The court in *Friendfinder* explicitly rejected the Ninth Circuit's reasoning, stating that the plain language of § 230(e)(2) exempted right of publicity claims and that this was "the general consensus before . . . *Perfect 10*."[64] It additionally noted that allowing such claims to survive would not "have a 'devastating' impact on the [I]nternet," and that "both the [I]nternet and so-called 'e-commerce' remain alive and well, and show no signs of imminent collapse."[65] The Ninth Circuit has determined that § 230 immunizes ISPs against the right of publicity, but in most jurisdictions this remains an open question.

The right of publicity grew out of the right to privacy,[66] which was originally devised to protect an individual's right to be "let alone."[67] The progenitors of the right to privacy identified the emotional harm caused by unwanted public exposure and argued that it should be a compensable injury.[68] They argued that privacy rights were neither contractual nor property rights but rather "rights as against the world."[69] The right of publicity was an expansion of the right to privacy, covering cases where public figures sought relief for unwanted public exposure.[70] Finding damage due to infringement of the right to be "let alone" seemed nonsensical when applied to

61. 488 F.3d 1102 (9th Cir. 2007).

62. *Id.* at 1119.

63. *Id.*

64. *Friendfinder*, 540 F. Supp. 2d at 301.

65. *Id.*

66. Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CALIF. L. REV. 127, 167 (1993) ("The right of publicity was created not so much from the right of privacy as from frustration with it.").

67. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 200 n.2 (1890).

68. *Id.* at 193, 197.

69. *Id.*

70. Mark P. McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U. PITT. L. REV. 225, 228 (2005).

plaintiffs, such as celebrities, who had made a career of seeking public exposure.[71] Thus, the right of publicity was based on appropriation of one's identity rather than on its public exposure, and it is distinguishable from other privacy rights in that respect—that is, the basis of harm is in the loss of economic associative value in the individual's identity.[72] But despite the right of publicity's basis in the underlying market value of identity, the majority of courts do not distinguish plaintiffs based on that value.[73] The majority view is that "non-celebrities have a right of publicity" despite the very low economic associative value of their identities.[74] Likewise, many commentators suggest that Lockean labor theory[75] is the proper theoretical mechanism for justifying right of publicity claims and distinguishing claimants.[76] Yet this theory, though generally accepted, is problematic when compared to the functional application of the right of publicity discussed in Part IV.A.

2. Defamation, Libel, and Intermediary Liability

Defamation predates the right to privacy, and it is also implicated in most cases of online identity misappropriation.[77] Contrary to disagreement about § 230's application to the right of publicity, courts agree that § 230 immunizes ISPs against defamation claims.[78] The elements of a defamation claim vary slightly but usually consist of "(1) a false and defamatory statement concerning another; (2) an unprivileged publication to a third-party; (3) fault

71. *Id.*

72. *Id.*

73. J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 4:16 (2d ed. 2000).

74. *Id.*

75. McKenna, *supra* note 70, at 230.

76. *See* Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L.J. 383, 388 (1999) (arguing that the theoretical basis for the right of publicity is that economic value in identity should be allocated to a claimant because the value is primarily the result of the claimant's own labor).

77. *E.g.*, Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006).

78. Ben Quarmby, *Protection from Online Libel: A Discussion and Comparison of the Legal and Extrajudicial Recourses Available to Individual and Corporate Plaintiffs*, 42 NEW ENG. L. REV. 275, 282 n.24 (2008); *cf.* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142 (Ct. App. 2004) ("We agree with appellants that the statute cannot be deemed to abrogate the common law principle that one who republishes defamatory matter originated by a third person is subject to liability if he or she knows or has reason to know of its defamatory character. By construing section 230 as conferring an absolute immunity, the trial court erred." (emphasis omitted) (citation omitted)), *rev'd*, 146 P.3d 510 (Cal. 2006).

amounting at least to negligence on the part of the publisher; and (4) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[79] Defamation law recognizes the torts of libel, for defamatory statements published in a fixed medium, and slander, for spoken defamatory statements.[80] Because online speech occurs in a fixed medium, defamatory online speech is considered libel.[81]

Under libel law, there are two ways to hold an intermediary liable. The first is publisher liability,[82] which holds that "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it."[83] Traditionally publisher liability applied to newspaper publishers, book publishers, broadcasters, and the like.[84] Courts applied liability to these publishers because the publishers commonly had a good deal of editorial control and discretion over content.[85] This editorial review process has resulted in a public perception that the publishers or broadcasters had "adopted the [defamatory] statements as [their] own."[86] Section 230 expressly provides immunity to ISPs from liability as a publisher.[87]

The alternative form of intermediary libel liability is distributor liability. Distributor liability differs from publisher liability in that distributors are considered passive in the conveyance of the defamatory statement since there is no editorial process.[88] Thus, a distributor is liable for the transmission of a defamatory statement only if the distributor "knows or has reason to know of its defamatory character."[89] Section 230 does not explicitly provide

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

80. BLACK'S LAW DICTIONARY 934, 1421 (8th ed. 2004).

81. *See* Glenn Harlan Reynolds, *Libel in the Blogosphere: Some Preliminary Thoughts*, 84 WASH. U. L. REV. 1157, 1164–65 (2006) (noting that some scholars argue online speech, particularly blogging, should be regarded as slander rather than libel).

82. RESTATEMENT (SECOND) OF TORTS § 578 (1977).

83. *Id.*

84. Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 144 (2008).

85. *Id.* at 144–45.

86. *Id.* at 145 (alteration in original).

87. 47 U.S.C. § 230(c)(1) (2006).

88. RESTATEMENT (SECOND) OF TORTS § 581(1) (1977).

89. *Id.*

immunity to ISPs from distributor liability. Indeed, it does not mention distributor liability.

Finally, common carriers such as telephone companies have traditionally been immune from liability.[90] Common carriers usually cannot control the statements transmitted over their networks and are required to serve all customers.[91] Therefore, courts have typically held that common carriers cannot be liable for the defamatory statements of others made over their networks.[92] Despite some similar characteristics, ISPs are not considered common carriers because they can refuse to serve customers.[93]

Zeran v. America Online, Inc.[94] established the contemporary interpretation of CDA immunity, granting broad protection from liability to ISPs.[95] The court went beyond the plain language of the statute in interpreting the breadth of immunity and construed it to include immunity for distributors as well as publishers.[96] Thus, under *Zeran*, even when an ISP or OSP has notice of tortious content on its server or webpage, it has no obligation to remove that content.[97]

Unlike the right to privacy and right of publicity, defamation did not develop as a positive right to be "let alone" or to control one's identity; rather, it developed as a negative right against "an assault on a person's reputation," which was considered "an assault on the entire community."[98] The First Amendment does not protect defamatory speech.[99] Nonetheless, First Amendment protections compel substantial limits on state defamation laws to protect against the possible chilling effect on speech that such laws may engender.[100] This policy consideration contributes to courts' reasoning that § 230

90. Ciolli, *supra* note 84, at 145.

91. *Id.*

92. *Id.*

93. *Id.* at 146.

94. 129 F.3d 327 (4th Cir. 1997).

95. *Id.* at 332.

96. *Id.*

97. *Id.*

98. Kate Silbaugh, Comment, *Sticks and Stones Can Break My Name: Nondefamatory Negligent Injury to Reputation*, 59 U. CHI. L. REV. 865, 866 (1992).

99. Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942).

100. Ciolli, *supra* note 84, at 159.

ought to be construed as broadly as possible in the defamation realm.[101]

B. Section 230 of the CDA and ISP Immunity

The CDA was passed in response to rising concerns about the availability of pornography online as the Internet developed.[102] It took two divergent approaches to policing online content: (1) a direct set of government-enforced criminal limitations on online activity, which the Supreme Court struck down within a year of the statute's enactment;[103] and (2) a hands-off, Internet exceptionalist approach of § 230, which survives today.[104] Congress passed § 230 for two stated reasons: first, to protect "Good Samaritan[]" ISPs and OSPs "who take[] steps to screen indecency and offensive material for their customers"; and second, to establish a policy against online content regulation by the federal government.[105]

There are two immunity provisions in § 230.[106] The first protects providers or users of Internet services (ISPs or OSPs) from treatment as a publisher or a speaker with regard to information posted by another content provider.[107] The second gives immunity to providers or users who make a good faith effort to restrict others' access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" content.[108] Section 230 was passed as a direct response to the ruling in *Stratton-Oakmont, Inc. v. Prodigy Services, Co.*,[109] where an ISP was held liable as a publisher because it had been vetting its online content of obscene materials.[110] The statute was passed specifically to overrule *Stratton-Oakmont*, in the

101. *See* Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003) ("[C]ourts construing § 230 have recognized as critical in applying the statute the concern that lawsuits could threaten the 'freedom of speech in the new and burgeoning Internet medium.'" (quoting *Zeran*, 129 F.3d at 330)).

102. Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 249 (2007).

103. Reno v. ACLU, 521 U.S. 844, 849, 885 (1997).

104. Medenica & Wahab, *supra* note 102, at 251–52.

105. 141 CONG. REC. 22,045 (1995) (statement of Sen. Cox).

106. 47 U.S.C. § 230(c) (2006).

107. *Id.* § 230(c)(1).

108. *Id.* § 230(c)(2)(A).

109. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Telecommunications Act of 1996, Pub. L. No. 104-104, sec. 509, § 230, 110 Stat. 56, 137.

110. *Id.* at *5.

hopes of encouraging ISPs to pursue their own online-content regulation and explore methods and technologies for protecting users from dangerous or obscene content.[111] Since its passage § 230, though initially intended to encourage ISPs to self-regulate, has become a shield from liability even when ISPs attempt no regulation whatsoever—immunizing them even when they work against content regulation of any kind.[112]

Zeran v. America Online, Inc. was decided a year after Congress passed the CDA.[113] The case concerned postings on an America Online (AOL) message board that advertised T-shirts with slogans expressing support for the Oklahoma City Bomber.[114] The shirt sales were fraudulently attributed to Ken Zeran.[115] Facing a high volume of angry calls, and even death threats, Zeran requested that AOL take down the posts, but despite AOL's efforts, the posts remained online.[116] Zeran therefore sued AOL for "unreasonable delay" in removing the posts.[117] Zeran attempted to work around § 230 publisher immunity by arguing that AOL was subject to distributor liability because it had notice of the defamatory posting.[118] The court dismissed Zeran's argument, however, stating that distributor liability was "merely a subset . . . of publisher liability, and is therefore also foreclosed by § 230."[119] The court went on to explain that in defamation law the distinction between distributors and publishers relates only to when liability attaches—before or after notice.[120] However, irrespective of when liability attaches, the court reasoned that any liable intermediary is liable as a publisher; § 230, therefore, applies to every intermediary ISP.[121]

111. H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 10, 208.

112. Medenica & Wahab, *supra* note 102, at 252.

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

114. *Id.* at 329.

115. *Id.*

116. *Id.*

117. *Id.* at 328.

118. *Id.* at 329–31.

119. *Id.* at 332.

120. *Id.* at 331–32.

121. *Id.* at 332 (citing W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113, at 802 (5th ed. 1984)).

Zeran laid out a three-part test for establishing immunity that has since become the predominant interpretation of § 230.[122] The ISP must show that (1) it acted as a user or provider of an interactive computer service; (2) the plaintiff seeks to hold it liable "as the publisher or speaker" of information furnished "by another information content provider"; and (3) it was not the "information content provider" of the content at issue.[123] The *Zeran* court precluded distributor liability despite the lack of any explicit statutory language to support this determination and, in so doing, possibly went beyond Congress's original intent.[124]

After *Zeran*, the Ninth Circuit further expanded the scope of immunity by expanding the definition of who or what qualifies as an ISP.[125] In *Batzel v. Smith*,[126] the court ruled that "the definition of 'interactive computer service' on its face covers 'any' information services or other systems, as long as the service or system allows 'multiple users' to access 'a computer server.'"[127] The defendant intermediary was the manager of an email listserv who had forwarded allegedly defamatory email messages to the listserv.[128] The court found the listserv manager immune as an ISP under § 230.[129] Similarly, in 2006, the California Supreme Court held in *Barrett v. Rosenthal*[130] that republishing information did not make one an information content provider.[131] It found that although the defendant had no actual supervisory role in operating the Internet site on which she had posted an allegedly defamatory email, she was nonetheless held to be immune as an ISP and OSP.[132]

122. Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 586 (2008). However, the opinion is not without controversy. *See* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 154 (Ct. App. 2004) ("The view of most scholars who have addressed the issue is that *Zeran*'s analysis of section 230 is flawed . . ."), *rev'd*, 146 P.3d 510 (2006).

123. *Zeran*, 129 F.3d at 330.

124. Ciolli, *supra* note 84, at 149–50.

125. Batzel v. Smith, 333 F.3d 1018, 1030 (9th Cir. 2003).

126. *Id.*

127. *Id.*

128. *Id.* at 1021.

129. *Id.* at 1032.

130. Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006).

131. *Id.* at 515.

132. *Id.*

The legislative history does not indicate whether Congress intended the immunity granted to ISPs to likewise apply to Internet users, webpage creators, and general posters of third-party-created content in the sense applied in *Barrett*.[133] Indeed, the *Barrett* panel itself noted that "[i]ndividual Internet 'users' like Rosenthal . . . are situated differently from institutional service providers with regard to some of the principal policy considerations discussed by the *Zeran* court and reflected in the Congressional Record."[134] Users are not faced with the volume of third-party postings that providers are and, furthermore, self-regulation for users is "far less challenging."[135] Nonetheless, the court extended immunity.

To understand courts' persistence in broadly construing § 230 immunity, it is important to consider the policy underlying the CDA's initial passage. The CDA was enacted in 1996 because Congress feared that the available communications laws were out of date and failed to cover the rapidly expanding Internet.[136] It was enacted to regulate indecency on the Internet and originally included only proactive regulatory measures prohibiting distribution of obscene materials online to minors.[137] Section 230 was proposed for the same purpose but with a different philosophy—a carrot to the proactive measures' stick—to encourage ISPs to take the initiative in self-regulation of obscene and offensive materials.[138] The statute itself proclaims this intention "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[139] In addition to this policy purpose, Congress also expressed an intention "to promote the continued development of the Internet and other interactive computer services and other interactive media [and] to preserve the vibrant and competitive free market . . . unfettered by Federal or State regulation."[140]

133. Ciolli, *supra* note 84, at 152.

134. *Barrett*, 146 P.3d at 526.

135. *Id.*

136. 141 CONG. REC. 15,502 (1995) (statement of Sen. Exon).

137. *See* Reno v. ACLU, 521 U.S. 844, 858–61 (1997).

138. Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997).

139. 47 U.S.C. § 230(b)(5) (2006).

140. *Id.* § 230(b)(1)–(2).

Following *Zeran*, courts have interpreted Congress's intent behind the CDA solely to favor freedom and deregulation in online policy, and they have done so at the expense of Congress's equally stated intention to fight online obscenity, stalking, and harassment. As a result, courts have nearly extinguished protections against online harassment and stalking, and they have allowed the killer combination of ISP immunity and user anonymity to all but eliminate safeguards and recourse for online conduct.[141] This one-sided policy results in a "user beware" Internet.

Rather than directly address the problems spawned by broadly construed § 230 immunity, courts have made exceptions in limited circumstances.[142] However, these exceptions are ineffective to combat the problem of broad immunity. For example, in *Barnes*, the case discussed in this Note's Introduction, the exception that the Ninth Circuit established actually weakened user identity protection with its promissory estoppel exception.[143] The court reasoned that estoppel liability survived § 230 because it was sufficiently distinct from publisher liability.[144] An ISP in the Ninth Circuit now risks losing § 230 immunity if it discusses the possibility of removing offensive content with a complaining victim.[145] Though this was a victory for Barnes, it was a blow to future victims of online identity misappropriation. The ruling in *Barnes* discourages ISPs from responding to victims of misappropriation about potentially infringing or offensive posts lest the ISPs open themselves to

141. *See, e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105–06 (9th Cir. 2009); Batzel v. Smith, 333 F.3d 1018, 1034 (9th Cir. 2003).

142. *See* Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1175–76 (9th Cir. 2008) (holding an ISP liable for third-party content when its online application form for housing induced posters to enter unconstitutionally prejudicial content); *see also* Stayart v. Yahoo! Inc., 651 F. Supp. 2d 873 (E.D. Wis. 2009) (allowing an exception for state "right of publicity" claims predicated on the statutory intellectual property exception from § 230(e)(2)). *But see* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1108 (9th Cir. 2008) (holding that immunity must be broadly construed to ensure courts do not "undermine" the immunity provided by the CDA).

143. *Barnes*, 570 F.3d at 1109. Barnes brought two claims in her complaint against Yahoo: negligent undertaking and promissory estoppel. *Id.* at 1098. The court dismissed the first but permitted the second. *Id.* at 1105–06, 1109.

144. *Id.* (noting liability came "not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happen[ed] to be removal of material from publication").

145. *Id.* at 1107.

liability.[146] In this way, the exception further frustrates victims' ability to compel ISPs to remove infringing content.

Some commentators have suggested that courts' tendency to make exceptions to broad immunity reveals a trend away from "Internet exceptionalism."[147] The majority opinion in *Fair Housing Council v. Roommates.com*[148] states that the Internet is "no longer a fragile new means of communication," but that it has "become a dominant—perhaps the preeminent—means through which commerce is conducted," reaching into "the lives of millions."[149] The court concluded that, therefore, it "must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their [offline] counterparts."[150] Courts ought to heed this warning and take such precautions.

C. Subpoena Law

As a matter of free speech, authors have a First Amendment right to remain anonymous.[151] In *Reno v. ACLU*,[152] the Supreme Court confirmed that this protection extends to online speech, noting that "democratic forums" online would be hindered if users could not maintain anonymity.[153] Consequentially, courts are cautious about compelling the unmasking of anonymous online posters. Unfortunately, there is no uniform standard for issuing a subpoena to an ISP compelling disclosure of a poster's identity ("John Doe subpoenas").[154] Different jurisdictions have different tests.[155]

146. Ali Grace Zieglowsky, *Immoral Immunity: Using a Totality of the Circumstances Approach to Narrow the Scope of Section 230 of the Communications Decency Act*, 61 HASTINGS L.J. 1307, 1330 (2010).

147. Varty Defterderia, Fair Housing Council v. Roommates.com*: A New Path for § 230 Immunity*, 24 BERKELEY TECH. L.J. 563, 583 (2009) ("The *Rooommates.com* majority no longer sees fit to extend the notion of cyber exceptionalism.").

148. 521 F.3d 1157 (9th Cir. 2008).

149. *Id.* at 1164 n.15.

150. *Id.*

151. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995).

152. 521 U.S. 844 (1997).

153. *Id.* at 868.

154. *See* Jason C. Miller, *Who's Exposing John Doe? Distinguishing Between Public and Private Figure Plaintiffs in Subpoenas and ISPs in Anonymous Online Defamation Suits*, 13 J. TECH. L. & POL'Y 299, 245–46 (2008).

155. *Id.*

Under the Federal Rules of Civil Procedure and in state courts that have adopted those rules, a victim must discover the identity of a third-party poster before he or she can proceed with a suit. However, in the types of cases addressed by this Note, the third-party poster has been anonymous. Because Rule 26(f) generally requires that the parties confer before a plaintiff may seek discovery, a victim-plaintiff can satisfy this requirement only by filing an ex parte motion seeking a subpoena compelling the ISP to disclose the poster's identity.[156] This motion is necessary because an ISP cannot legally disclose its users' identities without a court order.[157]

Most courts require court approval to issue a subpoena to a fictitiously named John Doe.[158] A plaintiff who wishes to subpoena a John Doe must submit an order to show cause that includes the reasons that the defendant should be identified.[159] Then the defendant's ISP informs the defendant of the order, and he or she can fight it anonymously through his or her attorney if he or she so chooses.[160] Once the plaintiff has submitted the order and the defendant has had an opportunity to respond, the court will determine whether the anonymous defendant's identity should be disclosed.[161] The amount and type of information that the plaintiff must submit in order to prevail on the motion depends on what standard the court uses to assess the merits of unmasking.[162] There is great variation in what courts require, and there are seven different major John Doe subpoena standards that courts have distinctly identified and used.[163] Five of these standards are applicable and will be discussed here.

In 1999, *Columbia Insurance Co. v. Seescandy.com*[164] provided the earliest decision on this issue and developed the first of these

156. *See, e.g.*, McMann v. Doe, 460 F. Supp. 2d 259, 262–63 (D. Mass. 2006).

157. 47 U.S.C. § 551(c)(2)(B) (2006).

158. Ryan M. Martin, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 U. CIN. L. REV. 1217, 1227 (2007).

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.* at 1227–33.

163. Nathaniel Gleicher, Note, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 YALE L.J. 320, 337, 339 (2008).

164. 185 F.R.D. 573 (N.D. Cal. 1999).

standards.[165] The court in *Seescandy* sought to balance the defendants' First Amendment rights against the injured parties' rights to seek recovery.[166] The court also noted that "limiting" principles must be applied to ensure that plaintiffs are not permitted to unmask anonymous speakers through frivolous suits simply to harass or embarrass innocent parties.[167] Each subsequent standard imposed on the issuance of John Doe subpoenas for anonymous online speakers has sought to balance these factors. How a court weighs these contravening concerns determines how difficult it will be for a plaintiff to unmask a Doe defendant and jurisdictions have balanced these concerns differently resulting in a range of standards.

The early standards that courts issued favored plaintiffs' interests over protection for anonymous online speakers.[168] In *Seescandy*, the plaintiff sought a John Doe subpoena to unmask an anonymous alleged trademark infringer.[169] The *Seescandy* test required only that the plaintiff (1) show that his or her case was strong enough to survive a motion to dismiss; (2) show that the information sought was likely to identify the defendant and, therefore, was relevant to the claim; and (3) disclose all steps taken to locate the defendant and show that a good faith effort had been made to serve the defendant.[170] The first two factors of the *Seescandy* test, assessing the strength of the plaintiff's case and the relevance of the information sought, are also found in each subsequent standard.

In re Subpoena Duces Tecum to America Online, Inc.[171] established a second standard that was even more favorable to plaintiffs than the *Seescandy* test.[172] *America Online* was the first notable defamation case to address whether a John Doe subpoena can be issued to an anonymous Internet poster.[173] The court applied a

165. *Id.* at 573.

166. *Id.* at 578 (noting that courts must consider "the need to provide injured parties with a forum in which they may seek redress for grievances," but stating that "this need must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously").

167. *Id.*

168. Gleicher, *supra* note 163, at 341.

169. *Seescandy.com*, 185 F.R.D. at 575–76.

170. *Id.* at 578–79.

171. No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000), *rev'd sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

172. *Id.* at *8.

173. Lynch, *supra* note 40, at 19.

three-pronged test: (1) the court must be "satisfied by the pleadings"; (2) the party seeking the subpoena must have a "good faith basis" for the assertion that his or her allegations were actionable; and (3) the disclosure of the identity must be "centrally needed to advance the claim."[174] This deferential standard required only that the plaintiff's claim be adequately specific, the defendant's identity be adequately relevant, and the claim itself be made in "good faith."

The *Rocker Management LLC v. John Does 1–20*[175] court took a stance far less deferential to plaintiffs than the standards of *Seescandy* and *America Online*.[176] The court used a totality-of-the-circumstances test to assess the merits of the plaintiff's claim.[177] The court noted the "grammar and spelling errors" on the forum in which the allegedly tortious statements had been posted, and it highlighted a forum warning message that postings therein were solely users' opinions.[178] Based on these findings, the court determined that a reasonable reader would not interpret the John Doe's forum posts to have been factual assertions and, as such, the claim for libel could not be successful.[179] The defendants' identities remained undisclosed.[180] *Rocker* heavily favors defendants by increasing the threshold requirements that the plaintiff must meet.[181]

The first standard to include an explicit balancing test and a notice provision was set forth in *Dendrite International v. Doe, No. 3*.[182] In *Dendrite*, the anonymous poster had posted purportedly inside information about a company on an online message board.[183] The court dismissed the "good faith" approach of *America Online* and laid out a four-part "sufficient evidence" approach.[184] Under this new approach, plaintiffs must first make an effort to notify the John Doe of the pending subpoena and allow sufficient time for the

174. *America Online*, 2000 WL 1210372, at *8.

175. No. 03-MC-33, 2003 WL 22149380 (N.D. Cal. May 29, 2003).

176. *Id.* at *3.

177. *Id.* at *2.

178. *Id.*

179. *Id.* at *2–3.

180. *Id.* at *3 (granting motion to quash subpoena seeking disclosure of defendants' identities).

181. *Id.*

182. 775 A.2d 756, 759–60 (N.J. Super. Ct. App. Div. 2001).

183. *Id.* at 762–63, 767.

184. Lynch, *supra* note 40, at 21–22.

defendant to file an opposition.[185] As an example, the court suggested that posting the notice on the message board where the offensive content had initially appeared would be sufficient.[186] Second, plaintiffs must present to the court the exact statements allegedly made by the anonymous poster.[187] Third, like in *Seescandy*, plaintiffs' pleadings must be able to survive a motion to dismiss; however, a greater showing is required under *Dendrite* than is required under *Seescandy*.[188] Under *Dendrite*, plaintiffs must produce "sufficient evidence" in support of each prima facie claim.[189] Finally, the court weighs the necessity for identity disclosure in light of each plaintiff's case against each defendant's First Amendment interest in anonymity.[190] In applying this standard to the case, the *Dendrite* court ruled that the plaintiff had failed to produce sufficient evidence and, as such, the court would not compel disclosure of the defendant's identity.[191] *Dendrite*, like *Rocker*, favors anonymous defendants. It allows courts to consider concerns not addressed by earlier standards and permits judicial flexibility in determining a proper balance, particularly in the face of "rapidly evolving technology."[192] Courts have frequently used the *Dendrite* test to bar plaintiffs' actions against John Does.[193]

The fifth standard—and the third one that heavily favors speaker anonymity—was established in *Doe v. Cahill*.[194] The court refused to adopt an approach similar to that in *America Online* or *Seescandy*, finding that the standards they set forth were "too easily satisfied" to adequately protect anonymous speech.[195] Instead, the court adopted a standard akin to that in *Dendrite*, but made it a two-prong test, combining the balancing and disclosure-of-allegedly-tortious-

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

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.* at 760–61.

191. *Id.* at 771.

192. Gleicher, *supra* note 163, at 340.

193. Donato v. Moldow, 865 A.2d 711, 714–15 (N.J. Super. Ct. App. Div. 2005) (holding that government officials failed to meet their burden, required by *Dendrite*, so as to compel disclosure of the defendants responsible for potentially defamatory political speech).

194. 884 A.2d 451 (Del. 2005).

195. *Id.* at 458.

statements prongs into the sufficient-evidence prong of *Dendrite*.[196] The *Cahill* court articulated its two-prong test as a summary judgment standard. The first prong is a notice requirement akin to that in *Dendrite*, and the second prong requires the plaintiff to present sufficient evidence to withstand a motion for summary judgment for each element of his or her claim—a "sufficiency of evidence" standard.[197] The court also made an exception for prima facie elements that would be nearly impossible to prove without disclosing the defendant's identity, such as the malicious-intent element required in a public figure's defamation claim.[198] The *Cahill* test, like that of *Dendrite*, weighs so heavily in favor of protecting anonymous speech that it seriously hinders the protection of Internet users who are victims of identity misappropriation.

Most courts have adopted a John Doe subpoena standard that is balanced heavily in favor of the anonymous online speaker, such as the *Dendrite* "sufficient evidence" standard or the *Cahill* "summary judgment" standard.[199] For example, in *Krinsky v. Doe 6*,[200] the court used a hybrid *Cahill-Dendrite* standard.[201] The court recognized that the notice prong, as expressed in *Cahill*, may now be "unrealistic and unprofitable" given the nature of today's Internet and given that an ISP will often notify the Doe defendant, as in *Krinsky*, when it receives a request for his or her identity.[202] The court also noted that there was too much variation from jurisdiction to jurisdiction in the application of *Cahill*'s summary judgment standard and, instead, applied a standard requiring "a prima facie showing of the elements" strong enough to overcome a motion to quash the subpoena seeking disclosure of the defendant's identity.[203]

These efforts to delineate a comprehensive standard for John Doe subpoenas attempt to balance multiple concerns. When courts

196. *Id.* at 461.

197. *Id.* at 463.

198. *Id.* at 462–63.

199. Lynch, *supra* note 40, at 26. *But see* Enterline v. Pocono Med. Ctr., No. 3:08-cv-1934, 2008 WL 5192386, at *5 (M.D. Pa. Dec. 11, 2008) (utilizing an *America Online*–type "good faith" standard but adding a comparative prong where the plaintiff must provide "information sufficient to establish or to disprove that claim or defense is unavailable from any other source").

200. 72 Cal. Rptr. 3d 231 (Ct. App. 2008).

201. *Id.* at 244–45.

202. *Id.* at 244.

203. *Id.* at 245.

use a standard that too heavily favors one side or the other, they risk eliminating the non-favored rights.[204] Weak protections for anonymity may allow plaintiffs to undertake "extra-judicial self-help remedies" after unmasking defendants.[205] Conversely, granting anonymity too much deference will immunize defendants, eliminate deterrence, and leave plaintiffs powerless.[206] Courts consider anonymity most critical in circumstances such as "governmental whistle blowing; labor organizing; dissident movements in repressive countries; gay and lesbian issues; and resources dealing with addiction, alcoholism, diseases and spousal abuse," as well as where the speech at issue contributes to important public debate.[207] Any standard designed to protect anonymous speech online should be particularly tailored to protect these kinds of speech. Protection covering speech outside of these particular circumstances, however, seriously risks eliminating a plaintiff's ability to fight against anonymous speech that is used to terrorize and harass.

III. CRITIQUE OF EXISTING LAW

A. Walled Garden to Web 2.0

ISPs and OSPs hold the key to individual autonomy in online identity construction. They have the power and capacity to control the flow and distribution of information online. Indeed, Congress designed the CDA to facilitate freedom for ISPs with this very fact in mind. However, the CDA was passed in 1996, and *Zeran* was decided in 1997. Since then, the Internet landscape has vastly changed, and the nature of ISP and OSP control over online information flow has changed with it. The expansive *Zeran* interpretation of CDA immunity no longer effectively upholds Congress's purpose in passing the act. The Internet of the 1990s was ISP-driven, self-contained, "read only," and accessible only to a minority of the population. Today's Internet is ubiquitous, interactive, user-driven, and integral to societal participation in

204. *See* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (holding that the CDA plainly immunizes ISPs and OSPs from liability for information that originated with third parties).

205. Doe v. Cahill, 884 A.2d 451, 457 (Del. 2005).

206. *See Zeran*, 129 F.3d at 334.

207. Gleicher, *supra* note 163, at 329 (citations omitted).

political, professional, financial, and social realms. As a result, it is imperative that ISPs and OSPs be subject to limited distributor liability—lest the law be read to incentivize lawlessness online.

Only 36 million people worldwide—0.9 percent of the world's population—used the Internet in 1996, the year the CDA was enacted.[208] Today, there are over 227 million Internet users in the United States alone, 77.3 percent of the U.S. population.[209] During this period of rapid growth, the Internet has changed in both size and structure. When the CDA was passed, the online landscape's structure was described as the walled garden web.[210] That is, the browsing environment of the 1990s "control[led] the information and Web sites the user [wa]s able to access."[211] ISPs like CompuServe and AOL provided a self-contained environment within which users could surf.[212] The ISPs designed their systems and services to direct users to supported content, creating a self-contained, walled-like network of webpages and applications within which most users remained throughout their online experience[213] At AOL's peak, 85 percent of its subscribers never left the confines of AOL's "garden."[214] On such services, web users "observed, found, and exchanged content passively . . . and privately, e.g., by emailing or engaging in person-to-person instant messages."[215]

By contrast, today's Internet is highly searchable, very versatile, and extremely interactive. The advent of broadband brought down the walled garden dial-up system of Internet provision. Unlike ISPs of the walled garden era, broadband companies seek to provide Internet access alone, divorced from regulating or providing

208. *Internet Growth Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/emarketing.htm (last visited Jan. 19, 2010).

209. *Internet Usage and Population in North America*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats14.htm (last visited June 30, 2010).

210. *Walled Garden*, WEBOPEDIA.COM, http://www.webopedia.com/TERM/W/walled_garden.html (last visited Jan. 19, 2010).

211. *Id.*

212. Ciolli, *supra* note 84, at 166, 183–84.

213. *Id.* at 167.

214. Richard Williamson, *Net Revolution Poised to Pounce on TV*, ZDNET AUSTRALIA (Apr. 5, 2001), http://www.zdnet.com.au/news/business/soa/Net-revolution-poised-to-pounce-on-TV/
0,139023166,120213824,00.htm.

215. Ziniti, *supra* note 122, at 590.

content.[216] They place few limits on the content accessible to users. Also, through broadband, the Internet is accessible twenty-four hours a day. In 2007, over 50 percent of U.S. households had broadband service,[217] and 79 percent of adults went online for an average of eleven hours a week.[218] These numbers have only increased.[219] Phenomena such as blogging and social networking, as well as web services like Google, YouTube, and Wikipedia, have revolutionized the way Internet content is created, organized, collected, and viewed and the way online communities are formed and developed. Additionally, hardware, such as iPhones and Blackberries, have made the Internet portable and accessible in ways unanticipated fifteen years ago.

This interactive Internet environment, dubbed "Web 2.0,"[220] "specializes in [building] community" through its services.[221] It is designed to "harness network effects" and improve as more people participate.[222] In contrast to ISPs' services in the walled garden era, Web 2.0 services are usually in the form of websites created and maintained by users and OSPs rather than in the form of content and sites created and maintained by the broadband ISPs themselves.[223] Additionally, Web 2.0 user interaction is increasingly public. Even one-to-one interactions are recorded and broadcast for public comment and collection by other users.[224] Users broadcast their real-world whereabouts and activities in real time from mobile devices and personal computers.[225] They create profile pages describing

216. Ciolli, *supra* note 84, at 173.

217. Stan Beer, *U.S. Residential Broadband Penetration to Exceed 50% in 2007*, ITWIRE (Feb. 18, 2007), http://www.itwire.com/it-industry-news/market/9666-us-residential-broadband-penetration-to-exceed-50-in-2007.

218. Solarina Ho, *Poll Finds Nearly 80 Percent of U.S. Adults Go Online*, REUTERS (Nov. 5, 2007, 8:35 PM), http://www.reuters.com/article/internetNews/idUSN0559828420071106.

219. Lance Whitney, *Average Net User Now Online 13 Hours Per Week*, CNET NEWS (Dec. 23, 2009, 7:30 AM), http://news.cnet.com/8301-1023_3-10421016-93.html (citing polls finding that 80 percent of adults go online 13 hours per week).

220. O'Reilly, *supra* note 3.

221. Ciolli, *supra* note 84, at 179.

222. Tim O'Reilly, *Web 2.0 and Cloud Computing*, O'REILLY RADAR (Oct. 26, 2008), http://radar.oreilly.com/2008/10/web-20-and-cloud-computing.html.

223. Ciolli, *supra* note 84, at 179; Ziniti, *supra* note 122, at 590.

224. *How News Feed Works*, FACEBOOK, http://www.facebook.com/help.php?page=408 (last visited Oct. 25, 2009).

225. *What Is Twitter?*, THEPICKY.COM, http://www.thepicky.com/internet/what-is-twitter-features (last visited Oct. 25, 2009).

themselves and their activities,[226] and they join networks that link them to professional connections where they can be rated and promoted to others.[227] They broadcast and rate their consumption of books, movies, and other media on sites that track users' likes and dislikes. Applications on these sites make automated recommendations based on users' tastes, and send this information along to participating friends and connections.[228] The rise of Web 2.0 has revolutionized not only the mode of interaction and expression online but also the very nature and function of users' online identities.

In the walled garden web, user identity, at best, comprised a "crabbed description," no more than a collection of statements or statistics.[229] It was far from the "highly nuanced and richly instantiated selves we experience in more social and interactive . . . environments."[230] The online identities of Web 2.0 users are much more akin to and have many more implications on our real-world identities than the walled garden Internet for which the *Zeran* protections were sufficient. One's online persona can be accessed by and has influence on one's social network, including friends, family, and acquaintances, as well as one's professional network, including colleagues, clients, employers and employees—both current and potential (in many fields, a clean and prominent Internet presence is essential for professional success).[231] A person's online persona is also accessible by and influential on advertisers, businesses, and various personalized service applications that are designed to integrate with and particularize to a person's identity. As online

226. *See* Aidan Henry, *Is Facebook Replacing E-mail?*, MAPPING WEB (July 11, 2007), http://www.mappingtheweb.com/2007/07/11/facebook-email.

227. *See LinkedIn*, WIKIPEDIA, http://en.wikipedia.org/wiki/LinkedIn (last visited Oct. 25, 2009).

228. *See, e.g.*, AMAZON, http://www.amazon.com/ (last visited Oct. 25, 2009) (making customized purchasing suggestions based on users' tastes); BLOCKBUSTER, http://www.blockbuster.com/ (last visited Oct. 25, 2009) (making customized movie suggestions based on users' tastes); NETFLIX, https://www.netflix.com/ (last visited Oct. 25, 2009) (making customized movie recommendations based on users' tastes).

229. Susan P. Crawford, *Who's in Charge of Who I Am?: Identity and Law Online*, 49 N.Y.L. SCH. L. REV. 211, 214 (2004).

230. Beth Simon Noveck, *Trademark Law and the Social Construction of Trust: Creating the Legal Framework for Online Identity*, 83 WASH. U. L.Q. 1733, 1746 (2005).

231. Ciolli, *supra* note 84, at 154 ("[A]n increasing number of employers now use the Internet to dig up potential dirt on their prospective hires during the interview process." (internal quotation marks omitted)).

identity has become more comprehensive and more closely tied to a user's real-world identity, the nature of online identity construction has remained versatile in its mutability and, therefore, vulnerable to co-opting, infringement, and fraud.

Congress could not predict the development of the Web 2.0 Internet, and the courts did not consider a system of this kind when they construed § 230 immunity so broadly. Under the *Zeran* system, there are no special provisions or incentives for ISPs or OSPs to protect the integrity of users' identities or to facilitate users' control over their identities. But ISPs, to some degree, and OSPs, generally, provide services that encourage and trade off of individualized user networking, socializing, and identity data collecting.[232] The outcome of broad immunity is that ISPs and OSPs, which are in the best position to control takedown and editing of user-created content and identity construction, have little legal incentive to regulate this content or to protect users. ISPs and OSPs, particularly, benefit greatly in the Web 2.0 environment by encouraging users to create and maintain online content;[233] yet § 230 immunity continues to provide them with nearly complete freedom from liability for harm to users caused by manipulation of their platforms and services. Users, therefore, bear the burden and cost. Because the general success of the Web 2.0 Internet depends on user interaction and participation, Congress's intention to encourage innovation, development, and expansion of the online marketplace of ideas is best served by providing a safe environment for users to control and develop their online personas without fear of misappropriation. This could be accomplished by rethinking the courts' interpretations of broad ISP immunity and allowing limited protection for users in particular cases.

B. Online Anonymity Protections

Overbroad immunity, when applied to Web 2.0, facilitates identity misappropriation like never before. Additionally, wide-

232. Ziniti, *supra* note 122, at 592 ("Services like photo-sharing and community site Flickr, or Amazon.com's community ratings system, take inputs from millions of users in the form of ratings, tags, and engagement (e.g., via analyzing what and how much users click, comment on, or forward to their friends) to make the online experience better.").

233. *Id.* at 592–93 (giving as an example, "services like Google's AdSense, which enables anyone with a blog to make money by hosting Google ads on it").

reaching protections for online anonymity embolden identity appropriators and harassers, as these perpetrators are not called to account for the repercussions of their actions.[234] The pairing of these features has led to increased levels of harassment.[235] Likewise, perpetrators' exclusively virtual encounters with their victims—many never meet their victims in *real* life—make the victims appear to harassers as mere images for manipulation.[236] These factors are exacerbating harassment online. This increase in online harassment is compounded by the lack of uniformity in John Doe subpoena law and the resulting difficulty in identifying and holding anonymous Internet actors liable under the prevalent standards discussed *supra* Part II.C.

In addition to the legal difficulty in obtaining a subpoena, there is a technical hurdle to overcome as well. Many ISPs and OSPs only store IP addresses—which could be necessary to identify a John Doe—for a period of sixty days or so.[237] This limited time frame requires a victim to act very quickly against a misappropriator if the victim hopes to compel the misappropriator's identification. It might help remedy this issue to instate a liability scheme against ISPs and OSPs that would enforce procedures for (1) notice and takedown of infringing posts and (2) longer-term maintenance of IP addresses for users. Takedown procedures would also help preserve online anonymity, because plaintiffs would be less likely to undertake the difficult process of seeking to unmask third-party posters if they had a more immediate remedy.[238]

At the time of the walled garden Internet, anonymity was a bedrock aspect of Internet culture.[239] A culture of anonymity and

234. Citron, *supra* note 29, at 83.

235. Michele L. Ybarra et al., *Examining Characteristics and Associated Distress Related to Internet Harassment*, 118 PEDIATRICS 1169 (2006), *available at* http://pediatrics.aappublications.org/cgi/content/abstract/118/4/e1169 ("[T]here has been a significant increase in the prevalence of Internet harassment from 2000 to 2005."); *Oldest Online Safety Organization Discloses Current Cyberstalking Statistics*, NET CRIMES & MISDEMEANORS BLOG (Apr. 29, 2009, 11:32 AM), http://www.netcrimes.net/2009/04/oldest-online-safety-organization.html ("Both Male and Female harassers in 2008 were about dead even for the 2nd year in a row[.] In 2008 an increase in victims aged 18–30, from 28% to 35%, was seen while 41+ aged victims increased from 29% to 32%[.]").

236. Citron, *supra* note 29, at 83.

237. Plaintiffs' Memorandum, *supra* note 43.

238. *See supra* Part II.C.

239. Lee Tien, *Symposium: Innovation and the Information Environment: Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117, 126–27 (1996).

pseudonymity—focused on "representation" rather than on "reputation"—predominated, and real-world identity was downplayed.[240] Because online identity is as alienable as it is mutable, Internet users may have a variety of different identities online, embedding themselves in different groups and playing different roles.[241] However, there has been a shift away from this culture in the Web 2.0 environment, which has been largely driven by technological advances.[242] Software capabilities now go beyond the "mere naming conventions" typical of walled garden identity builders, such that individuals can now "create positive and robust" online personas.[243] Thus, the modern focus of online identity is reputation because reputation integrates peoples' online and offline identities.

Where courts administer tougher standards for John Doe subpoenas, they do so in the name of protecting free speech online.[244] But the freedom to speak anonymously should not be the only free speech consideration. The potential chilling effect on online speech that may result from weaker protections for anonymity is not more problematic than are the chilling effects on online speech that may result from weak protections for those who had chosen to speak using their own voices in their real-world identities. Just as an individual's right to speak anonymously is integral to his or her freedom of speech, so too is his or her right to open self-expression. He or she should not be forced to speak anonymously nor be subject to someone else putting words in his or her mouth.

Also, anonymity can have negative effects on speech. One school of thought holds that people are more prone to behave aggressively when they believe they cannot be seen or will not be caught.[245] This tendency has led to aggressive online harassment that targets women, children, and minority groups. It has also led victims to leave Internet discourse or resign their identities online (real or pseudonymous) and take on anonymity.[246] As some scholars have

240. Noveck, *supra* note 230, at 1751.

241. *Id.* at 1746–47.

242. *Id.* at 1751.

243. *Id.*

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

245. Citron, *supra* note 29, at 81–82.

246. *Id.* at 82, 85.

argued, the right to anonymous speech may be "better termed a 'qualified privilege.'"[247] Anonymous speech whose primary purpose is to impede or eliminate others' rights to self-expression should not be privileged.[248] Because proper functioning of the Web 2.0 Internet depends on users maintaining consistent identities, with many users using their real-world identities for this purpose, the freedom to speak anonymously online must be weighed against the needs of Web 2.0 users to manage and control the consistency of their online presence and self-expression. In some circumstances, other rights outweigh the right to anonymity. Here, it should be outweighed by the individual's right to speak with his or her own voice and preserved online by securing such individuals' integrity of identity.

C. Victim Recourse Under Current Law

Misuse and misappropriation of identity are common tactics in online harassment.[249] Harassers gain access to personal and personally identifying information, either through Web searches of publicly accessible information or through actual invasions of privacy, by hacking into victims' computers or email accounts.[250] The acquired information is then posted online, either in a tone purporting that the harasser is the individual whose information is being posted, or in a way that otherwise invites third parties to misuse or misappropriate the information or correlating identity.[251] Once the victim discovers such a posting, he or she must contact the ISP or site OSP to request that the post be taken down.[252] The victim is then subject to the whim of the ISP or OSP with respect to removal. Furthermore, unless the OSP's actions or the victim's claim fits within very limited exceptions that vary by jurisdiction, the OSP is immune from liability for the post and for any failure to remove it. Meanwhile, the posted material remains active, exposing the victim to further danger from and harassment by third parties. During this time, "[v]ictims feel a sustained loss of personal security and

247. Gleicher, *supra* note 163, at 327 (noting that the right to anonymity "is better termed a 'qualified privilege'").

248. STEVEN J. HEYMAN, FREE SPEECH AND HUMAN DIGNITY 166 (2008).

249. *See* Citron, *supra* note 29, at 61, 63–64.

250. *Id.* at 70.

251. *Id.*

252. *Id.*

regularly dismantle their online presence[s] to avoid further devastation of their privacy."[253]

For recourse against an anonymous poster, a victim must first contact the OSP for the website where the material was initially posted. The victim must request identifying information (if any was taken) or the IP address of the poster in hopes of tracing it to the poster's real-world identity.[254] The OSP may not have identifying information for the third-party poster, as OSPs are not obligated to retain this information. If the OSP does have the information the victim must compel its disclosure by court order through filing for a John Doe subpoena.[255] A court will not issue this subpoena unless it determines that the victim can meet one of the various standards of review, depending on the rule in that jurisdiction.

At this point, if not before, the anonymous poster will be given notice of the victim's efforts to unmask him or her, and he or she will have an opportunity to respond with an opposition brief to quash the subpoena. The court will then make another determination on the subpoena. If is the court issues the subpoena, the victim may proceed on various tort grounds against the poster. Until this time, however, the victim will have no recourse for his or her injury, and he or she will have no leverage to remove the offending post.

IV. PROPOSAL

A. The Online Right to Autonomy of Identity

An individual's interest in "autonomous self-definition" is a central issue to any solution posed by cases like *Barnes*.[256] In this respect, the right of publicity is the only right to autonomy of identity that courts have recognized as an exception to § 230 immunity.[257] But to fall within this exception, a victim must show that the misuse or misappropriation of the victim's identity was made "for purposes of trade or advertising."[258] This severe limitation on the scope of

253. *Id.*

254. *Id.*

255. *Id.*

256. *See* McKenna, *supra* note 70, at 231 (analyzing the history and reasoning behind the right to privacy and concluding that "[a]ll individuals have a legitimate interest in autonomous self-definition").

257. *See* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 292, 303 (D.N.H. 2008).

258. Cohen v. Herbal Concepts, Inc., 472 N.E.2d 307, 308 (N.Y. 1984).

infringement for which a victim can recover does not adequately account for the "emotional and economic" costs borne by victims whose interests in autonomous self-definition have been violated.[259] Though the state-law right of publicity as it stands today is inadequate to sufficiently protect user identity, the historical and theoretical underpinnings of the right of publicity tend to justify a right to autonomous self-definition.[260] Moreover, the nature of the Web 2.0 environment necessitates a limited recognition of this right in order to protect the Internet users' safety and interests and to uphold Congress's intent in passing § 230—to protect the integrity, vitality, and diversity of the online community.

Since 1890 when Samuel Warren and Louis Brandeis first proposed that the right to privacy ought to be protected, it has become "one of the broadest concepts in the law," supporting a wide array of interests and fostering little consensus as to its meaning as a legal concept.[261] Unfortunately, courts have viewed identity misappropriation through the lens of privacy. As a result, they have considered it in light of Warren and Brandeis's initial premise that the right to privacy found its basis in the individual's fundamental interest in being "let alone."[262] However, claims regarding identity misappropriation are ill suited to this theoretical basis. Victims of identity misappropriation are not typically trying to be let alone to hide from public view. Rather, a victim is typically seeking to create a public image that the misappropriation undermines or contradicts.[263] It was this kind of discrepancy that led to the creation of the right of publicity to begin with, in that being let alone did not fit the goals of public figures who were simultaneously seeking publicity in their own right.[264]

The right of publicity was premised on a theory analogizing one's right in one's identity to a property right.[265] However, property theory cannot adequately justify the right of publicity, as celebrity is

259. McKenna, *supra* note 70, at 229.

260. *Id.* at 229, 232–33.

261. *Id.* at 238–39.

262. Warren & Brandeis, *supra* note 67, at 193.

263. *See, e.g.*, O'Brien v. Pabst Sales Co., 124 F.2d 167, 170 (5th Cir. 1941).

264. McKenna, *supra* note 70, at 228.

265. *Id.* at 234–35.

not a scarce resource in need of protection.[266] Likewise, labor theories "overstate an individual's role in the creation of any economic value in his or her public persona,"[267] and the appropriation of a celebrity's identity may be no more likely to exhaust the value of his or her identity than it is to increase the value.[268] After all, as the adage states, all publicity is good publicity. Additionally, courts often apply the right of publicity in instances where plaintiffs have done nothing to cultivate their personas' economic value and do not have an economic interest in exploiting whatever value their personas may hold.[269] For these reasons, application of the right of publicity seems to be predicated not so much on the appropriation of economic value in identity but on appropriation of identity itself. If so, its key theoretical underpinning seems to be a right of autonomy of identity.[270]

Claims such as those in *Barnes* and *Perfect 10, Inc.* should be premised on this fundamental theory. In those cases, the harm caused to the victim was not simply economic: it was harm to functional reputation, to the right of self-expression, to personal safety and security, and to the ability to participate freely online without obstruction. Furthermore, those harms did not stem solely from the fraudulent posts themselves but also from the failures to effectively remove them from the Internet. ISPs and OSPs today make money from Web 2.0's identity-based participatory structure but do not shoulder their share of the burden in terms of liability.[271] Courts should adopt a policy with respect to ISP immunity that recognizes the right to autonomy of identity as a state intellectual property exception like the right of publicity. This would maximize protection for victims and shift some of the burden to protect against infringement onto those in the best position to remedy its harm

266. *Id.* at 273–74.

267. *Id.* at 252.

268. *Id.* at 265 (providing an excellent and thorough analysis).

269. *See* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 292 (D.N.H. 2008) (allowing a claim for violation of the right of publicity for a plaintiff who did not trade off of her identity or image).

270. McKenna, *supra* note 70, at 229.

271. Ziniti, *supra* note 122, at 593, 595.

through takedown. Such recognition would ensure better protection for online speech,[272] Internet participation, and Internet development.

B. Limited Exception to ISP Distributor Liability

Protection for the integrity of user identity is essential to Internet development and the development of other related interactive media and technology in the Web 2.0 era.[273] Likewise, protections for "online discourse" and "cultural development,"[274] which go hand in hand with protections against stalking and harassment online, are dependent on protection of user identity in Web 2.0.[275] Therefore, for courts to accomplish Congress's stated intention for § 230, they must rethink the *Zeran* interpretation of § 230.[276]

Attempts to roll back § 230 immunity in order to remedy its inadequate protection have rarely been upheld[277] and have been decried by commentators as a "deviation from the clearly stated goals of [the] statute and the accompanying consistent judicial interpretation."[278] Such commentary regards any encroachment on broad § 230 immunity as an affront to the beneficial policy of Internet exceptionalism, presumed to be central to the congressional policy underlying the CDA.[279] Such criticism, however, overlooks the fact that courts initially granted broadened immunity that encompassed distributor liability as an expansion *beyond* the bounds

272. Citron, *supra* note 29, at 83, 97 ("One of free speech's most important functions is promoting individual autonomy.").

273. *See* 47 U.S.C. § 230 (2006).

274. Noveck, *supra* note 230, at 1733, 1750 (noting that a "robust online identity . . . is essential to successful commerce and society online").

275. 47 U.S.C. § 230(b).

276. Ziniti, *supra* note 122, at 601 ("Courts could implement a knowledge-triggered liability system without congressional action by reverting to the common law distributor liability standard.").

277. *See* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 142 (Ct. App. 2004) (ruling that an ISP ought to be subject to liability as a distributor when the ISP has been given notice of a tortious posting and has received a request to remove it, but has failed to do so), *rev'd*, 146 P.3d 510 (2006).

278. Defterderia, *supra* note 147, at 579 (reasoning that Congress intentionally chose to relieve ISPs from the liability scheme applicable to their real-world publisher and distributor counterparts because such liability would be potentially damaging to the continued growth and development of the Internet).

279. Eric Goldman, *The Third Wave of Internet Exceptionalism*, TECH. & MARKETING L. BLOG (Mar. 11, 2009, 12:20PM), http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm (defining Internet exceptionalism as a policy of "crafting internet specific laws that diverge from regulatory precedents in other media").

of the statutory language of § 230 for the purpose of accomplishing congressional intent.[280] However, Congress did not necessarily intend this expansion.[281] As such, a rollback of broad immunity, bringing the breadth of ISP immunity more in line with the statutory language of § 230, would accomplish Congress's initial stated intent and respect congressional authority. Indeed, minor exceptions to broad § 230 immunity do not sufficiently protect Internet users' identities. Only wholesale elimination of immunity for notice-based distributor liability in those circumstances where a victim's identity has been co-opted will effectively protect victims of identity misappropriation.

Therefore, courts ought to recognize a particular exception from the general rule interpreting § 230 as immunizing ISPs and OSPs against distributor liability. ISPs and OSPs should be subject to notice-based liability for negligence in cases where (1) a third-party poster fraudulently misappropriates another user's identity and makes a post *as* that individual (not merely *about* that individual);[282] (2) the user whose identity has been subjected to misappropriation has given the ISP or OSP notice that the posting is reasonably viewed as a misappropriation of his or her identity; and (3) the user requested that the posting be taken down. Critics may argue that any opening in ISP and OSP liability for third-party posting will chill online discourse,[283] yet other nations, such as Britain and Ireland, do not offer immunity to ISPs, and those countries still benefit from "vibrant online discourse."[284]

Also, a distinction must be drawn between OSPs, which have control over the content on a particular website, and ISPs, such as broadband providers, which function more like common carriers and do not directly control webpages or platforms for public-content posting. ISPs that function like common carriers should not be

280. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

281. *Id.* ("Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to § 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact.").

282. However, violations should include the posting of personal data, such as personal contact information, a Social Security number, or credit card numbers, that subjects an individual to real-world danger.

283. *See* Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 112 (2007) (noting of the reasoning behind immunity that "if Internet intermediaries were liable every time someone posted problematic content . . . the resulting threat of liability . . . would debilitate the Internet").

284. Citron, *supra* note 29, at 120 (citation omitted).

subject to distributor liability because Congress's intent would not be furthered by removing *Zeran* immunity in these cases. However, because OSPs control content and are in the best position to protect Internet users from prolonged harm to their rights to autonomous self-definition and integrity of identity, OSPs ought to have a duty to take down the content in a reasonable amount of time. This duty should arise where the OSP has actual knowledge that material is reasonably infringing and the victim provides notice to the OSP.[285] The requirement that the victim provide notice to the OSP will safeguard OSPs against a duty to police every claimed violation and will ensure that the victim is, in fact, taking an active role in the construction and maintenance of his or her online identity. Lastly, a safe-harbor provision limiting this liability should also be enforced, though this may require congressional action, as no such provision is written into the CDA.

C. Notice and Takedown Safe-Harbor Provision

Although, under the current system, a victim of identity misappropriation may bring suit directly against the third-party poster as recourse for damage done, such recourse has become increasingly difficult for reasons beyond those already discussed. There is software now on the market that allows users to "hide (or in the alternative, continuously change) their IP addresses."[286] As use of such software increases, a plaintiff's ability to unmask an anonymous poster may become nearly impossible. Even without this technological advance, a third-party poster can avoid detection and eliminate the possibility of recourse against him or her by posting the material from a computer that does not identify him or her.[287] Likewise, even when a victim obtains a subpoena, unmasks and successfully sues the third-party poster, the harm will not have been eliminated because the post will have already been spread online over search archives, Internet caches, or in the original post (when the OSP refuses to dismantle it).[288] Because such posts remain

285. It is important to note that the requirement of both actual knowledge and proper notice protects OSPs from liability where they had reason to know but did not receive proper notice, as warned against in Ziniti, *supra* note 122, at 601.

286. Quarmby, *supra* note 78, at 291–92.

287. *See* Doe v. Friendfinder Network, Inc., 540 F. Supp. 2d 288, 292 (D.N.H. 2008).

288. Citron, *supra* note 29, at 83, 84 ("Their refusal can stem from a libertarian 'You Own Your Own Words' philosophy, or irresponsibility bred from the belief that they enjoy broad

viewable, they can, as in *Barnes*, serve as a "call[] to action" for more harassment.[289] Therefore, even successful suits for damages against third-party posters will seldom be adequate remedies for victims. Furthermore, studies have shown that most plaintiffs would prefer to simply have the offending posts removed than to get money damages.[290] Seventy-five percent of libel plaintiffs say they would have refrained from litigation if they had received a retraction, correction, or apology.[291] Therefore, enforceable means of identity protection that require OSPs to take down identity-misappropriating posts would be more effective to remedy online infringement than the current suit-for-damages system.

Such a system would require limited notice-based liability for OSPs. However, liability for failure to take down posts should trigger only when the notice has been properly provided. The Digital Millennium Copyright Act (DMCA) serves as a good model for determining appropriate notice.[292] Under the DMCA, a copyright holder must give written notification of claimed copyright infringement, identify the copyrighted work, identify the material claimed to be infringed, provide contact information for the copyright holder/victim, give a statement of good faith belief, and include a signature and statement of accuracy under penalty of perjury.[293] Here, similar criteria for giving notice would be effective. As a preliminary matter, OSPs should be obligated to provide a means of contact by which notice can be filed. Only the victim or his or her agent should file notice with the OSP. The victim should be obligated to fill out a form certifying, on penalty of perjury, that (1) the victim is the individual whose identity has been appropriated in the offending post; (2) the victim has a good faith belief that the material in question has served to misappropriate his or her identity; and (3) the information in the victim's notification is accurate to the

statutory immunity from liability."); *see also id.* at 74 (citing the *AutoAdmit* case, Ciolli v. Iravani, No. 2:08-cv-02601, 2008 WL 4412053 (E.D. Pa. Sept. 23, 2008) (*AutoAdmit*), where "a site manager asserted that he would not remove the offensive threads until the female students apologized for threatening litigation").

289. *Id.* at 84.

290. Ciolli, *supra* note 84, at 238.

291. *Id.*; *see also id.* at 189 ("[S]eventy-five percent [of defamation plaintiffs] are motivated by non-monetary factors.").

292. 17 U.S.C. § 512(c)(1) (2006).

293. *Id.*

best of his or her knowledge. The victim should identify the particular elements of the post that arguably appropriate his or her identity and should therefore be removed. These specifications should be reasonably sufficient to permit the OSP to locate the material. The victim should offer reasonable documentation of how the elements of the post infringe on his or her identity. He or she should offer contact information reasonably sufficient to allow the OSP to contact him or her. If the OSP receives such notice, it would then have a reasonable duty of care to take down the offending post. Failure to exercise this reasonable duty of care should result in liability. Reasonable efforts to take down the offending material should result in safe harbor and immunity from suit. Of course, not all Internet media have easily manageable content.[294] For this reason, an OSP ought to be held only to a reasonable standard of care to make efforts to remove the infringing post in a reasonable time after receiving notice.

D. Safeguards Against Misuse

Scholars have noted that notice-and-takedown regimes such as ones like the DMCA's "have not worked well" because they may "sweep too broadly," causing OSPs to take down postings simply to avoid liability.[295] Likewise, OSPs may lose a good deal of time and money investigating complaints.[296] Such concerns are misplaced with respect to this proposed system, however, because they are narrowly drawn and personally driven. OSPs have no duty to remove simple references to an individual, nor are they duty-bound to remove allegedly defamatory postings that do not have third parties posing as the victim or giving out sensitive personal information. Also, individuals protecting their personal identities generally have less time and money than corporations protecting their intellectual property have. Individuals are therefore less likely to submit proper takedown requests to ISPs and OSPs for minor or questionable violations.

Additional concerns with requiring OSP responsibility for takedowns crop up with respect to identity misappropriation claims

294. Ciolli, *supra* note 84, at 253–54.

295. Citron, *supra* note 29, at 122.

296. Ciolli, *supra* note 84, at 260.

that stem from postings on sites that operate without a central administrator who has complete control over the website.[297] In such instances, the OSP is not in a position to easily remove infringing material. These concerns are alleviated by the fact that an OSP is only obligated to make a reasonable effort to remove the offending material.

E. Limiting Online Anonymity

OSP liability and a notice-and-takedown system would not completely alleviate the problem faced in *Barnes*, however. Because of the speed with which information spreads across the Internet, it is sometimes difficult to completely eliminate a harmful post.[298] For this reason, it is also important to place limitations on Internet anonymity. To this end, ISPs and OSPs should be obligated to trace identifying information on each anonymous poster. This way, online anonymity could be preserved while the destructive actions resulting from the lack of accountability in anonymity would be held in check.[299]

The technology for tracking anonymous Internet posters is already available and being used by ISPs and OSPs. ISPs routinely keep records of IP addresses for users.[300] In addition to IP addresses, many websites use a software component called a "cookie."[301] Because IP addresses often change, many OSPs use cookies to track users who access their sites from the same computer at different times.[302] Between cookies and IP-address tracking, the technological framework is in place for tracking anonymous posters. However, ISPs and OSPs are not obligated to collect and store this information for any particular length of time, and there is no guarantee that an anonymous user will be traceable. ISPs and OSPs should be obligated to retain this information for a definite period of time and should be liable for the loss of this information when a John Doe

297. *Id.* at 261.

298. *Id.* at 260–61.

299. Citron, *supra* note 29, at 124.

300. Doe v. Cahill, 884 A.2d 451, 454–55 (Del. Super. Ct. 2005).

301. Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 87–88 (2002) (noting that cookie software tracks user identity by communications from the website's server to the user's Internet browser and back again).

302. *Id.*

subpoena has issued so that there would be appropriate limits on anonymity. Such limits would abate the perception that harassers are untouchable.

In addition to obligatory ISP and OSP retention of user-identity data, Congress should establish a uniform system for issuing John Doe subpoenas. However, until this is accomplished, the takedown provisions for identity misappropriation that are suggested in this Note should satisfy even the more stringent *Dendrite* standard. Due to obligations on ISPs and OSPs, identity would be traceable in the case of alleged identity misappropriation. Thus, ISPs and OSPs would be able to give notice to a Doe defendant facing a subpoena. Likewise, if a plaintiff has issued appropriate notice and request for removal, then the notice, the sworn statement, and the additional information collected and presented to the OSP should support the claim against the Doe defendant.

Perhaps the greatest objection to traceable anonymity is that it constitutes de facto elimination of anonymity online and results in the hindrance of free speech. While this objection has merit, the methods and technology involved with tracing identity are already in place. The only change this Note suggests is a statutory obligation that ISPs and OSPs retain the information they are already tracking. Such an obligation may place a higher burden on smaller OSPs that allow third-party posting but do not actually track IP or cookie information. For these smaller OSPs, there are alternative methods for tracing identity. Many sites require registration by email in order to post. Such registration would suffice.

Violating a user's right to privacy online is the other great concern with imposing an obligation on ISPs and OSPs to collect information that could be used to create records of online activity. However, as Justice Douglas recognized, "[o]ne who enters any public place sacrifices some of his privacy."[303] Obligating ISPs and OSPs to retain identity-tracing data does not obligate them to track user activity or collect users' personal information. Most information gathered using cookies and IP addresses is anonymous because these do not convey any personal information in their own right.[304]

303. Pub. Utils. Comm'n v. Pollack, 343 U.S. 451, 468 (1952) (Douglas, J., dissenting).

304. Keck, *supra* note 301, at 90.

V. JUDICIAL AND LEGISLATIVE STEPS

This Note's proposals would require courts to overrule the *Zeran* interpretation of distributor liability. This revision would require no action by Congress because congressional intent with the CDA is already clear; it was the judiciary that first drew a broad line around all ISP liability from § 230. Coverage of distributor liability is not addressed in § 230, and policy considerations favor eliminating immunity in the limited case of negligence for OSPs that, after notice, fail to remove identity-misappropriating material. Thus, courts would have discretion to distinguish ISPs that are like common carriers from OSPs that regulate content. While requirements for reasonable notice and takedown in these cases could also come from the courts, Congress or state legislatures are better suited to the task.

This proposal's other elements require legislative action. Congress should obligate ISPs and OSPs to retain identity-tracing records. Such legislation would serve a number of purposes, including many beyond this Note's scope. The statute should place a duty of care on ISPs to retain basic identification records for a reasonable period of time. This duty would only attach to ISPs that permit third-party posting and only apply to those users who post content online. Such additions would fill the void left by Internet exceptionalism in protecting online identity.

VI. CONCLUSION

Changes in Internet technology and culture have led to an online environment wherein user identity is an integral part and a driving force in the Internet's discourse and development. As a result, it is imperative that courts rethink their approaches to CDA immunity and roll it back where it disfavors protections for the autonomy of Internet-user identity. Policy considerations—such as protections against harassment and stalking for users attempting to contribute and interact online—necessitate limits on online anonymity. ISPs are in the best position to aid users in regulating their online identities and to trace users who post infringing material. ISPs are also the greatest beneficiaries of Web 2.0's identity-driven system. Therefore, ISPs must be made to bear a greater portion of the burden to protect users and maintain an environment of safe interaction online.