SCALING BACK § 230 IMMUNITY: WHY THE COMMUNICATIONS DECENCY ACT SHOULD TAKE A PAGE FROM THE DIGITAL MILLENNIUM COPYRIGHT ACT'S SERVICE PROVIDER IMMUNITY PLAYBOOK

TABLE OF CONTENTS

I. INTRODUCTION

In September 2010, Craigslist closed the adult services section of its classified advertisements website.[1] The move came just one week after a group of attorneys general voiced concerns with the amount of ads promoting illegal prostitution within the online community.[2] Although forty state attorneys general previously contacted Craigslist concerning its screening efforts in 2008, the website came under heightened scrutiny following the suicide of a young man awaiting trial for the killing of a

1. *See Craigslist Removes Adult Services Section*, MSNBC.COM, http://www.msnbc.msn.com/id/39005873/ns/technology_and_science-tech_and_gadgets (last updated Sept. 4, 2010).

2. *See id.*

masseuse he met through Craigslist.[3]

This begs the question: Would Craigslist have been under any threat of liability had it refused to remove the ads? The answer is almost certainly no. Section 230 of the Communications Decency Act[4] (CDA) provides powerful protection for online service providers, such as Craigslist, when third-party users provide illegal content to the website.[5] This Note examines the shortcomings of the immunity provided by § 230 and proposes a solution to those shortcomings. Part II begins by surveying defamation law and its implications on the Internet. Part III looks at the history, criticism, and judicial treatment of § 230 of the CDA. Part IV looks to copyright law and its treatment of websites in the Digital Millennium Copyright Act (DMCA). Part V suggests a restructuring of the CDA so that its immunity more closely resembles the safe harbor provisions created by the DMCA.

II. DEFAMATION LAW AND ITS TREATMENT OF WEBSITES

A. *Traditional, Pre-Internet Defamation Law: Common Carrier Versus Distributor Versus Publisher*

The law of defamation—one of the oldest forms of damages recognized by most legal systems—was designed to protect individuals' reputations.[6] Despite the First Amendment's guarantee that "Congress shall make no law . . . abridging the freedom of speech or freedom of the press,"[7] the tort of defamation continues to provide recourse for individuals who have their reputations damaged due to the publication of defamatory statements.[8] Prior to the inception of the Internet, the nineteenth and twentieth centuries saw an entire body of defamation law develop, a majority of which involved the publishing of defamatory material in

3. *See id.*

4. Communications Decency Act (CDA) of 1996, 47 U.S.C. § 230 (2006).

5. *See id.*

6. *See generally* David S. Ardia, Comment, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 284 (2010).

7. U.S. CONST. amend. I.

8. Melissa A. Troiano, *The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447, 1452 (2006) (citations omitted).

newspapers.[9] Jurisdictions often reference the *Restatement* with regard to defamation or libel claims against print publications.[10] Such a claim requires the defamed to prove the following elements: "(a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting to at least negligence on the part of the publisher; and (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication."[11]

"Special conditions apply, however, where a plaintiff names not just the original speaker as a defendant, but also the publisher and distributor of the statement."[12] Under traditional defamation law principles, liability is determined by first distinguishing between common carriers, distributors,

9. *See, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (analyzing an allegedly defamatory editorial in the *New York Times*); Finnish Temperance Soc'y Sovittaja v. Publ'g Co., 130 N.E. 845 (Mass. 1921) (deciding a defamation lawsuit against a publishing company for publishing a libelous letter targeting a religious organization); Sweet v. Post Publ'g Co., 102 N.E. 660 (Mass. 1913) (deciding a defamation lawsuit against a publishing company for publishing an article falsely asserting the plaintiff, an attorney, was indicted for fraud); Farley v. Evening Chronicle Publ'g Co., 87 S.W. 565 (Mo. Ct. App. 1905) (deciding a defamation lawsuit against a publishing company for publishing an article describing the plaintiff as a violent enemy of the labor unions); Pellardis v. Journal Printing Co., 74 N.W. 99 (Wis. 1898) (deciding a defamation lawsuit against a publishing company for publishing an article falsely describing the plaintiff as a convicted criminal); Hanson v. Globe Newspaper Co., 34 N.E. 462 (Mass. 1893) (deciding a defamation lawsuit against a newspaper company for misspelling a convicted criminal's name, which falsely implied the plaintiff was the criminal); Burt v. Advertiser Newspaper Co., 28 N.E. 1 (Mass. 1891) (deciding a defamation lawsuit against a newspaper where it had published four allegedly false statements regarding the plaintiff).

10. *See, e.g.*, Moss v. Camp Pemigewassett, Inc., 312 F.3d 503, 507 (1st Cir. 2002) (citations omitted) (applying precedent, which relies on the *Restatement*, to a defamation claim); Beverly Enters., Inc. v. Trump, 182 F.3d 183, 188 (3d Cir. 1999) (quoting RESTATEMENT (SECOND) OF TORTS § 566 cmt. e (1977)) (using the *Restatement* to distinguish "vulgar name-calling" from defamation); Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (citing RESTATEMENT (SECOND) OF TORTS § 558(b) (1977)) (citing the *Restatement* for the proposition that a "publication of a statement is a necessary element in a defamation action"); Jesinger v. Nev. Fed. Credit Union, 24 F.3d 1127, 1133 (9th Cir. 1994) ("Nevada courts have relied on the Restatement (Second) of Torts to fashion appropriate rules in defamation cases." (footnote and citations omitted)).

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

12. John E.D. Larkin, *Criminal and Civil Liability for User Generated Content: Craigslist, a Case Study*, 15 J. TECH. L. & POL'Y 85, 102 (2010).

and publishers of information.[13] Common carriers, including telephone companies, have very little control over the content of the information communicated over their networks and thus are normally afforded immunity from liability for the defamatory statements transmitted by users.[14] Liability can only attach if a common carrier has reason to know that the sender of a defamatory message is not privileged to make the communication.[15] The passive nature of the common carrier justifies the provided immunity, as telephone companies generally serve as "a conduit for the expression of others."[16]

Because it is often easy to determine whether an entity is a common carrier[17] and the law is relatively well settled in the area, most of the non-Internet defamation litigation has addressed the distinction between distributors and publishers. According to the *Restatement*, distributors can be held liable for defamatory material only if they know or have reason to know of the material's defamatory character.[18] For instance, in *Smith v. California*,[19] the Supreme Court struck down a city ordinance that imposed strict liability on bookstores for the possession of publications containing obscene or indecent material.[20] The Court ruled that a distributor, such as a bookstore, must have knowledge of the contents of the writings before it can be held liable.[21] Concerned for "'constitutionally protected expression,'" the Court inferred that upholding the strict liability ordinance would cause bookstore owners to only sell books they have scrupulously

13. Jessica L. Chilson, Note, *Unmasking John Doe: Setting a Standard for Discovery in Anonymous Internet Defamation Cases*, 95 VA. L. REV. 389, 399 (2009); *see also* Bryan J. Davis, Comment, *Untangling the "Publisher" Versus "Information Content Provider" Paradox of 47 U.S.C. § 230: Toward a Rationale Application of the Communications Decency Act in Defamation Suits Against Internet Service Providers*, 32 N.M. L. REV. 75, 78–83 (2002) (distinguishing among the defamation standards for common carriers, distributors, and publishers).

14. Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 145 (2008) (citing Anderson v. N.Y. Tel. Co., 320 N.E.2d 647, 649 (N.Y. 1974) (Gabrielli, J., concurring)).

15. Davis, *supra* note 13, at 82.

16. Nicholas P. Dickerson, Comment, *What Makes the Internet So Special? And Why, Where, How, and by Whom Should Its Content Be Regulated?*, 46 HOUS. L. REV. 61, 88 (2009).

17. Davis, *supra* note 13, at 79 ("'Common carriers' include telephone, telegraph, and microwave communication services.").

18. RESTATEMENT (SECOND) OF TORTS § 581 (2010).

19. Smith v. California, 361 U.S. 147 (1959).

20. *Id.* at 148 n.1, 155.

21. *See id.* at 154–55.

examined, regardless of whether the publication contained indecent material.[22]

Due to their superior editorial control over the defamatory material, publishers are held to a higher standard of liability than their secondary publisher counterparts.[23] Publishers of third-party content possessing editorial control, such as a magazine, can normally be held liable for defamation when they are at least negligent in regard to the defamatory nature of the statement.[24] The Supreme Court first addressed publisher liability for defamation against a private individual in *Gertz v. Robert Welch, Inc*.[25] In *Gertz*, a magazine published a series of articles implying that a lawyer had a criminal record without seeking verification, while also accusing the lawyer of coordinating the conviction of a police officer in furtherance of the communist party's plan to supplant police departments.[26] The Court reversed the lower court's decision, which required knowledge or reckless disregard of the defamatory nature of the statement on the part of the publisher, and the Court increased the potential for publisher liability by lowering the standard of fault to negligence.[27] Thus, when the defamation involves a private individual, a publisher must have acted at least negligently in publishing the defamatory statement.

B. *Pre-CDA Internet Defamation Law*

As the age of newsprint publication collided with the inception of the Internet, courts attempted to retain symmetry between print publication and Internet defamation cases. One of the first early Internet defamation cases was *Cubby, Inc. v. CompuServe, Inc.*, where an individual was allegedly defamed in one of the online forums hosted by CompuServe.[28] The defamatory material was located in a newsletter that was posted to the website's Journalism Forum, one of 150 topics located in the database.[29] CompuServe had no opportunity to exercise editorial control over the

22. Davis, *supra* note 13, at 82 (quoting *Smith*, 361 U.S. at 153).

23. *See id.* at 80.

24. RESTATEMENT (SECOND) OF TORTS § 558(c) (2010).

25. Gertz v. Robert Welch, Inc., 418 U.S. 323, 325 (1974).

26. *See id.* at 325–26.

27. *Id.* at 349. The Court went on to state, "[S]o long as [States] do not impose liability without fault, the States may define for themselves the appropriate standard of liability for a publisher." *Id.* at 347.

28. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 137–38 (S.D.N.Y. 1991).

29. *See id.*

newsletter, as it was immediately available to subscribers when it was posted to the forum, nor did CompuServe compensate the user who posted the newsletter.[30]

While the plaintiff argued that CompuServe should be held to a publisher standard of liability, CompuServe maintained that a distributor standard of fault was appropriate.[31] As such, CompuServe contended that it could not be held liable "because it neither knew nor had reason to know of the allegedly defamatory statements."[32] The court agreed with CompuServe, likening the website's role in hosting the newsletter to that of a library.[33] In ruling that CompuServe should not be held liable for defamation, the court concluded that CompuServe had no more editorial control than "a more traditional news vendor," and it "would impose an undue burden on the free flow of information" if websites like CompuServe were asked to monitor every publication for defamatory material.[34] Because the plaintiff did not allege that CompuServe had knowledge or reason to know of the defamatory nature of the newsletter, summary judgment was granted for CompuServe.[35] Thus, the district court determined that the distributor liability doctrine found in *Smith* should also apply to online distributors such as CompuServe.[36]

Another early Internet defamation case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, applied the publisher standard to defamatory content created by a third party.[37] The defamatory statement at issue involved Stratton Oakmont, a securities investment firm, and was posted by an individual on a "Money Talk" bulletin board operated by the online service Prodigy.[38] Despite the federal district court's ruling in *Cubby*, the New York Supreme Court applied publisher liability to Prodigy due to the

30. *See id.*

31. *Id.* at 139.

32. *Id.*

33. *Id.* ("CompuServe's CIS product is in essence an electronic, for-profit library that carries a vast number of publications . . . .").

34. *Id.* at 140.

35. *Id.* at 141.

36. *See id.* at 139, 141.

37. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. IAS Part 34, 1995 WL 323710, at *4–5 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, 47 U.S.C. § 230 (1998), *as recognized in* Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d 1011, 1016 (N.Y. 2011).

38. *Id.* at *1.

substantial editorial control the website exercised.[39] The court offered two distinctions between Prodigy's operation of its bulletin board and the role of the service provider in *CompuServe*.[40] Prodigy not only "held itself out to the public . . . as controlling the content of its computer bulletin boards," but it also implemented an "automatic software screening program" to control the forum.[41] According to the court, Prodigy's use of technology and manpower to delete posts on the basis of offensiveness was sufficient for Prodigy to be considered a publisher for purposes of the defamatory newsletter.[42]

The *Cubby* and *Stratton Oakmont* decisions effectively encourage Internet service providers (ISPs) to ignore defamatory statements posted to websites and forego implementing monitoring systems. If an ISP chooses to police the website for defamatory material, it risks exercising editorial control and being subjected to the publisher liability standard.[43] In the alternative, if an ISP simply allows third parties to post statements freely without any supervision on the part of the website, only then can it be held to a distributor's standard of fault.[44] Faced with such a decision, an ISP almost certainly would not attempt to block defamatory content by monitoring the website in an effort to avoid becoming a "publisher" of the content. Recognizing this conflict, and in direct response to the *Stratton Oakmont* decision, Congress enacted § 230 of the CDA.[45]

III. COMMUNICATIONS DECENCY ACT: § 230

A. *The Passing of § 230 of the CDA*

"In an effort to remove the disincentives to self-regulation created by the decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, and to avoid the onslaught of litigation that would otherwise likely have ensued,

39. *See id.* at *4–5.

40. *See id.* at *4.

41. *Id.*

42. *Id.* at *5.

43. *See id.* at *4–5.

44. *See, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 137, 140–41 (S.D.N.Y. 1991).

45. *See* Ali Grace Zieglowsky, Note, *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, 1307 (2010); *see generally* 47 U.S.C. § 230 (1998) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

Congress passed § 230 of the Communications Decency Act in 1996."[46] Perhaps the most persuasive justification for website protection was the Internet's infancy at the time of the CDA's adoption.[47] Congress was fearful that holding websites liable for a third party's defamatory comments would subject the upstart web providers to exponential liability, stunting the growth of the Internet.[48] Therefore, Congress's stated intention was "to promote the continued development of the Internet" and "preserve the vibrant and competitive free market that presently exists for the Internet."[49]

The relevant portion of § 230 provides protection for "Good Samaritan" blocking and screening of offensive material and states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[50] The subsection also provides protection for websites that attempt to restrict users' access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material.[51] This provision explicitly overrules the holding in *Stratton Oakmont*.[52] The Internet was still in its developmental years when the law was passed, making it difficult for Congress to predict all potential applications of the section; thus, the Act leaves much to be interpreted by the courts regarding

46. Zieglowsky, *supra* note 45.

47. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) ("Congress recognized the threat . . . to freedom of speech in the new and burgeoning Internet medium.").

48. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1027–28 (9th Cir. 2003) (citations omitted) ("[L]awsuits could threaten 'the freedom of speech in the new and burgeoning Internet medium.'" (quoting *Zeran*, 129 F.3d at 330)); *Zeran*, 129 F.3d at 330 ("Congress recognized the threat that tort-based lawsuits pose[d]."); *see also* Stuart M. Riback, *Liability-Proofing Your Internet Presence*, CONSUMER FIN. L. Q. REP., Spring 2010, at 49, 49.

49. 47 U.S.C. § 230 (2006).

50. *Id.* § 230(c)(1).

51. *Id.* § 230(c)(2)(A).

52. *Compare id.* ("No provider . . . shall be held liable . . . [for] any action . . . to restrict access to or availability of . . . obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable [material]."), *with* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. IAS Part 34, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995) ("PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability."), *superseded by statute*, 47 U.S.C. § 230 (1998), *as recognized in* Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d 1011, 1016 (N.Y. 2011).

the scope of the protection.[53]

B. *Development of § 230's Immunity in the Courts*

In *Zeran v. America Online, Inc.*, the Fourth Circuit was provided with the first opportunity to examine the breadth of § 230's safeguard for websites.[54] The case involved a defamation claim brought by an individual, Zeran, who was allegedly defamed on a bulletin board maintained by America Online (AOL).[55] Specifically, a forum message advertising t-shirts with imprinted offensive slogans listed Zeran as the seller, including his telephone number.[56] After receiving numerous threatening phone calls from angry AOL users, Zeran contacted an AOL representative, informing the website provider of his predicament and requesting the post be taken down.[57] Several additional posts were made by the unidentified individual, further advertising the sale of various distasteful items.[58] Zeran subsequently brought a negligence action against AOL alleging the website provider failed to promptly remove the defamatory advertisements and to screen for similar future postings.[59]

The court of appeals upheld the district court's ruling, finding that § 230 of the CDA provided interactive computer service providers protection from all claims based on statements posted by third parties.[60] After explaining the purpose of Congress's enactment of § 230, the court addressed Zeran's argument that the protection provided by the CDA eliminates only publisher liability—and not distributor liability—for website providers.[61] Thus, Zeran argued a website provider with knowledge of the defamatory material can still be held liable as a distributor, despite § 230's Good Samaritan provision.[62] Siding with AOL, the court ruled § 230's use of the term "publisher" is not intended to extend distributors beyond its reach; instead, Congress merely intended to

53. *See* Zieglowsky, *supra* note 45, at 1311 (citations omitted).
54. *Zeran*, 129 F.3d 327.
55. *Id.* at 329.
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.* at 327–28.
60. *See id.* at 330–31.
61. *Id.* at 331. This argument was based on the wording of § 230, which provides that an ISP shall not be treated as the "publisher" of the statement, but makes no mention of distributors. *Id.* at 331–32.
62. *See id.*

use the term generally.[63] "In other words, even where plaintiffs could prove that defendant website operators 'had a high degree of awareness of [the statement's] probable falsity, or to have in fact entertained serious doubts as to the truth of his publication,' *Zeran* would deny relief."[64] Thus, the distinction between publisher and distributor illustrated in *Cubby* and *Stratton Oakmont* does not apply when interpreting § 230's Good Samaritan provision.[65]

Following the Fourth Circuit's declaration of a "federal immunity" in *Zeran*,[66] subsequent cases have clarified and broadened the protection provided to websites under § 230 of the CDA.[67] "Faced with the task of implementing Congress's aims and determining ISP liability, the courts did in fact interpret the statute broadly, believing such an interpretation to be in line with the statute's purpose of fostering free expression on the internet."[68]

Contributing to the rapid expansion of § 230 immunity was the U.S. District Court for the District of Columbia in *Blumenthal v. Drudge*, a case decided one year after *Zeran*.[69] In *Blumenthal*, the court extended § 230 immunity to an ISP that maintained a website featuring a defamatory "gossip" column.[70] The salient distinction in the case was that unlike the anonymous, independent user who posted the statements in *Zeran*, the writer of the defamatory material in *Blumenthal* was contracted with and paid by the ISP.[71] This fact was deemed irrelevant by the court, which stated, "Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others."[72] "Thus, even when defamatory content is developed at a service provider's request, the provider is immune from liability so long as it is not the author of the

63. *See id.* at 332–33.

64. Larkin, *supra* note 12, at 105 (quoting Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d Cir. 1984)) (alterations in original).

65. *See Zeran*, 129 F.3d at 332–33.

66. *Id.* at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.").

67. Zieglowsky, *supra* note 45, at 1312–14 (footnotes omitted).

68. *Id.* at 1311.

69. Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

70. *See id.* at 51, 53.

71. *See id.* at 51.

72. *Id.* at 52.

material."[73]

In *Batzel v. Smith*, the Ninth Circuit continued to stretch the coverage of § 230 immunity.[74] The case involved an online Museum Security Network that posted the contents of a letter accusing an individual of possessing stolen artwork.[75] The court ultimately remanded to determine whether the website should have "reasonably concluded" that the original writer of the letter did not intend for the information to be posted online.[76] Although this approach is certainly preferable to blindly granting § 230 immunity, the court would still allow a website to post unsubstantiated material absent any type of investigation into the information's legitimacy—so long as the website could have reasonably concluded that the original source intended for the information to be posted.[77]

Further contributing to the liberal interpretation of website immunity under § 230 was the Ninth Circuit in *Carafano v. Metrosplash.com, Inc.* Matchmaker.com (Matchmaker)—an online dating service that allows users to create a profile and use a drop-down menu to select one of several provided responses to questions concerning interests or appearance, such as "'looking for a one night stand'"—claimed immunity under § 230.[78] An unknown person constructed a profile depicting the plaintiff as a woman seeking a male counterpart.[79] The profile included the plaintiff's home address and an e-mail address, which automatically responded to any messages by providing the plaintiff's home address and telephone number.[80] Soon thereafter, the plaintiff began receiving harassing phone calls and sexually explicit messages.[81]

73. Gregory M. Dickinson, Note, *An Interpretive Framework for Narrower Immunity Under Section 230 of the Communications Decency Act*, 33 HARV. J.L. & PUB. POL'Y 863, 868 (2010).

74. Batzel v. Smith, 333 F.3d 1018, 1035 (9th Cir. 2003).

75. *Id.* at 1021–22.

76. *Id.* at 1035. According to the court, such a determination was necessary to establish whether the letter was actually "'provided by another information content provider'" under § 230. *Id.* at 1037 (Gould, J., concurring in part and dissenting in part) (quoting 47 U.S.C. § 230(c)).

77. *See id.* at 1038 ("Under the majority's rule, a court determining whether to extend CDA immunity to a defendant must determine whether the author of allegedly defamatory information . . . intended that the information be distributed on the Internet.").

78. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003).

79. *Id.*

80. *Id.*

81. *Id.*

The court extended § 230 immunity to the website, holding, "Matchmaker cannot be considered an 'information content provider' under the statute because no profile has any content until a user actively creates it."[82] Further, the court determined that, even assuming Matchmaker was acting as an information content provider, Carafano would have to establish that the website "created or developed the particular information at issue."[83] Given that the information at issue—Carafano's telephone number—was submitted directly by the user and not selected from a drop-down menu supplied by Matchmaker, Carafano would still be unable to defeat Matchmaker's defense of § 230 immunity.[84]

C. *Recent Refusal to Grant Absolute Immunity Under § 230*

Since Congress's adoption of § 230 of the CDA and its initial interpretation in *Zeran*, courts have provided nearly absolute immunity to ISPs when a third party is the creator of the defamatory material.[85] However, several courts have recently applied § 230 immunity more narrowly, resulting in websites being considered information content providers even when they are not the literal author of the material.[86]

One such court was the Ninth Circuit in *Fair Housing Council of San Fernando Valley v. Roommates.com*, which involved a discrimination claim against the website, Roommates.com (Roommates).[87] The purpose of the site is to assist renters of spare rooms in finding prospective occupants.[88] Subscribers are required to create a profile before being allowed to search listings or post housing opportunities.[89] Profiles not only include basic information, such as location and name, but also require subscribers to divulge their "sex, sexual orientation, and whether [they] would bring children to a household."[90] Users select the relevant responses from a list of answers provided by the website.[91] Alleging a violation of the federal Fair Housing Act, the Fair Housing Council of the San Fernando Valley

82. *Id.* at 1124.
83. *Id.* at 1125.
84. *See id.*
85. *See supra* Part III.B.
86. *See* Dickinson, *supra* note 73, at 875.
87. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).
88. *Id.* at 1161.
89. *Id.*
90. *Id.*
91. *See id.* at 1164, 1166.

and San Diego brought suit against the website.[92]

Declining to construe § 230 as broadly as *Zeran* and its progeny, the court refused to extend immunity to the housing website.[93] The court reasoned that "[b]y requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information."[94] Although the court failed to enumerate a specific standard describing when a website may be held liable for material provided by a third party, it did distinguish the case from its prior holding in *Carafano*, another drop-down menu case.[95] In *Carafano*, the court noted that although the individual used the website's neutral tools to publish the information, the libelous material was created and developed entirely by the user.[96] Alternatively, in *Roommates.com*, "Roommate both elicit[ed] the allegedly illegal content and [made] aggressive use of it in conducting its business."[97] The distinction seems to be, simply, that Roommates became an information content provider by essentially requiring users to engage in allegedly illegal conduct, whereas the website in *Carafano* "had nothing to do with the user's decision to enter a celebrity's name and personal information in an otherwise licit dating service."[98]

The Tenth Circuit also opted for a narrower reading of § 230 in *FTC v. Accusearch Inc.*, a case decided one year after *Roommates.com*.[99] Abika.com (Abika), a website that paid investigators to obtain private phone records that the website operator's knew to have been obtained illegally, sought and ultimately failing to obtain § 230 immunity.[100] The court held Akiba acted as an information content provider, making § 230 immunity unavailable.[101] "By paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by

92. *Id.* at 1162.
93. *See id.* at 1175.
94. *Id.* at 1166.
95. *See id.* at 1171 (citations omitted).
96. *Id.* ("The claim against the website was, in effect, that it failed to review each user-created profile to ensure that it wasn't defamatory.").
97. *Id.* at 1172.
98. *Id.*
99. FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).
100. *Id.* at 1191–92.
101. *Id.* at 1201.

law, it contributed mightily to the unlawful conduct of its researchers."[102] The court implied that § 230 immunity does not attach where a website creates a platform it "intends to be overwhelmingly filled with some identifiable illegal conduct."[103]

Shortly after the adoption of § 230, courts strictly perpetuated Congress's intentions in adopting the provision by granting broad immunity for ISPs.[104] According to courts interpreting § 230 in its infancy, any involvement in the creation of defamatory material short of authoring the content cannot create website liability.[105] Beginning with *Zeran*, courts have refused to hold an ISP liable when it has a "'high degree of awareness'" of the presence of defamatory material on the website.[106] Further, courts have generally held that ISPs have no affirmative duty to investigate or monitor websites for defamatory content.[107] However, two recent court decisions have revealed a narrowing of § 230 immunity.[108] The court in *Roommates.com* and *Accusearch* essentially established that § 230 will not attach if the ISP requires or encourages third parties to post infringing material.[109] However, an ISP must do something more than simply provide users with the means to commit defamation.

102. *Id.* at 1200.

103. Samuel J. Morley, *How Broad Is Web Publisher Immunity Under § 230 of the Communications Decency Act of 1996?*, FLA. B.J., Feb. 2010, at 9, 16; *see Accusearch*, 570 F.3d at 1199 ("[A] service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content.").

104. *See supra* Part III.B.

105. *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) ("[S]o long as the third party willingly provides the essential publishing content, the interactive service provider receives full immunity regardless of the specific editing or selection process.").

106. *See* Larkin, *supra* note 12, at 105 (quoting Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d Cir. 1984) (internal quotations omitted)).

107. *See, e.g.*, Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) ("Congress has conferred immunity from tort liability . . . , even where the self-policing is unsuccessful or not even attempted."); Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) ("It would be impossible for service providers to screen each of their millions of postings for possible problems.").

108. *See* FTC v. Accusearch Inc., 570 F.3d 1187, 1201 (10th Cir. 2009); Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1162 (9th Cir. 2008).

109. *See Accusearch*, 570 F.3d at 1201; *Roommates.com*, 521 F.3d at 1162.

D. *Criticisms of CDA § 230 Immunity*

Since the adoption of § 230 of the CDA, the protection provided by the provision has come under attack. The most cited criticism of § 230 is the broad interpretation of the immunity enumerated in *Zeran*.[110] The result of the *Zeran* decision is the immunization of "parties surely not within the intended scope of Section 230."[111] Notwithstanding the recent *Roommates* and *Accusearch* decisions, a website that encourages users to post others' credit card information and embarrassing stories would likely enjoy § 230 protection.[112] This is because the only requirement for § 230 immunity under *Zeran* is that the material originate with a third-party user.[113] *Zeran*'s construction of § 230 does not allow for situations where immunity should not be extended despite third-party authorship.[114]

Another criticism of the CDA's immunity provision is the failure of the section to achieve one of its main objectives. Although Congress's intent was to remove disincentives to self-regulation by ISPs—by encouraging ISPs to edit or post third-party material without fear of being regarded as the publisher of the material—§ 230 has failed to provide an incentive for websites to regulate.[115] Another claim by detractors of § 230 immunity is that the Internet is not the same as it was when § 230 was adopted, and consequently, websites no longer require as much special protection.[116] As stated earlier, in adopting § 230, Congress sought to protect the development of the Internet and avoid stunting its growth.[117]

110. *See, e.g.*, Dickinson, *supra* note 73, at 872–74 (criticizing the "*Zeran* line of cases").

111. *Id.* at 873.

112. *Id.*

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

114. *See* Dickinson, *supra* note 73, at 873 (noting that a hypothetical website, "harassthem.com," where users post true or fabricated personal information and defamatory content, could be structured to enjoy § 230 immunity under *Zeran*).

115. *See* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (discussing the inconsistency between § 230's caption and its judicial interpretation); *see also* J. Andrew Crossett, Un*fair Housing on the Internet: The Effect of the Communications Decency Act on the Fair Housing Act*, 73 MO. L. REV. 195, 202 (2008) ("[T]he title makes little sense when the effect of the section is 'to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services.'" (quoting *GTE Corp.*, 347 F.3d at 660)).

116. *See, e.g.*, Zieglowsky, *supra* note 45, at 1313–14 ("[W]e are no longer in the early stages of the internet's development. Congress created § 230 of the CDA based on a simplistic and utopian version of the internet . . . .").

117. *See supra* note 48 and accompanying text.

"Internet publications have matured to the point where, at least in certain instances, they are robust enough to face the same exposure to liability as their print counterparts."[118]

IV. COPYRIGHT LAW AND ITS TREATMENT OF WEBSITES

A. *Digital Millennium Copyright Act and Its Safe Harbor Provision*

Defamation is not the only area of law that has provided ISPs with some form of immunity from suits involving third-party content.[119] In fact, § 230 explicitly exempts intellectual property violations from its coverage.[120] The DMCA provides immunity, or a "safe harbor," similar to the one found in the CDA.[121] "When Congress passed the DMCA in 1998, it sought to provide a safe harbor against copyright liability for the normal operations of online service providers with respect to actions performed by users of its services."[122]

In order to enjoy the protections of a safe harbor, an online service provider (OSP) "must be a service provider as defined in § 512(k) and meet the threshold requirements under § 512(i) as well as the specific requirements under one of the [safe harbor provisions]."[123] Threshold requirements under § 512(i) include: "(A) the OSP must have adopted and reasonably implemented a policy for termination of repeat infringers; and (B) the OSP must not interfere with standard technical measures."[124] A more specific requirement is provided by § 512(c), which requires an OSP to lack knowledge of the infringement[125] and not receive financial benefit from the infringing activity,[126] to respond expeditiously to remove or

118. Dickinson, *supra* note 73, at 874 (citing Robert G. Magee & Tae Hee Lee, *Information Conduits or Content Developers? Determining Whether News Portals Should Enjoy Blanket Immunity from Defamation Suits*, 12 COMM. L. & POL'Y 369 (2007)).

119. *See, e.g.*, 17 U.S.C. § 512 (2006) (providing safe harbor provisions under copyright law).

120. *See* 47 U.S.C. § 230(e)(2) (2006).

121. 17 U.S.C. § 512.

122. Peter Brown, *Copyright Law and the Internet: The Evolution Continues*, *in* INTELLECTUAL PROPERTY LAW INSTITUTE 2010, 593, 600–01 (2010).

123. Liliana Chang, Note, *The Red Flag Test for Apparent Knowledge Under the DMCA §512(c) Safe Harbor*, 28 CARDOZO ARTS & ENT. L.J. 195, 199 (2010).

124. *Id.* (citing 17 U.S.C. § 512(i)(1)).

125. 17 U.S.C. § 512(c)(1)(A).

126. *Id.* § 512(c)(1)(B).

disable access to the infringing material upon notification,[127] and to have a designated agent to receive notifications.[128] Knowledge under the statute includes not only actual knowledge of the infringement but also apparent knowledge, where the OSP is "aware of facts or circumstances from which infringing activity is apparent."[129]

B. *Courts' Application of the DMCA Safe Harbor Provisions*

It requires little analysis to conclude the DMCA safe harbor provisions differ quite significantly from § 230's immunity granted under the CDA. Most salient of these differences is the DMCA's requirement that the OSP lack knowledge of the infringing material,[130] and the OSP's subsequent obligation to remove the material once notice has been given.[131] The cases discussed below demonstrate judicial treatment of the DMCA safe harbor provisions and of ISPs.

In *Arista Records LLC v. Usenet.com, Inc.*,[132] the court considered whether the provider of an online bulletin board where users regularly posted links to copyrighted articles and MP3 files was covered by the DMCA safe harbor provisions.[133] As a result of the website's active engagement in and knowledge of the uploading of infringing content, the court precluded the website from asserting the DMCA's safe harbor provisions.[134] The court ultimately held the defendant was not only a "secondary" copyright infringer but also a direct infringer, stating that the website was "not merely a 'passive conduit' that facilitates the exchange of content between users who upload infringing content and users who download such content."[135]

In *Perfect 10, Inc. v. CCBill* (*Perfect 10 II*), the Ninth Circuit denied an OSP the benefits of the DMCA safe harbor provisions because the website was not enforcing its DMCA policy.[136] In *Perfect 10, Inc. v. CCBill*

127. *Id.* § 512(c)(1)(C).
128. *Id.* § 512(c)(2).
129. *Id.* § 512(c)(1)(A)(ii); *see also* Chang, *supra* note 123, at 200–01.
130. 17 U.S.C. § 512(c)(1)(A).
131. *Id.* § 512(c)(1)(C).
132. Arista Records LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124 (S.D.N.Y. 2009).
133. *See id.* at 129–31, 133.
134. *See id.* at 148–49.
135. *Id.* at 149.
136. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1120–21 (9th Cir. 2007) [hereinafter "*Perfect 10 II*"].

(*Perfect 10 I*), the district court noted that "[t]he DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe."[137]

More importantly, the *Perfect 10* cases illustrate the courts' insistence that the burden to identify infringing material lies with the copyright holder and not the service provider.[138] The cases involved an entity, Cavecreek Wholesale Internet Exchange (CWIE), that provided webhosting and Internet connectivity services to various websites.[139] One of those websites posted copyrighted images stolen from Perfect 10's website.[140] Perfect 10 argued that CWIE was aware of the apparent infringing activities due to the incriminating titles of some of the websites, including "'illegal.net'" and "'stolencelebritypics.com.'"[141] Perfect 10 essentially argued that knowledge should have been imputed to CCBill as a result of certain "red flags," a principle enumerated by Congress in § 512 of the DMCA.[142] Under the "red flag test," a service provider cannot take advantage of the safe harbor provisions if it fails to remove infringing material when it is "aware of facts or circumstances from which infringing activity is apparent."[143] Disagreeing with Perfect 10, the court found that the names of the websites for which CCBill provided services did not create a red flag for purposes of the Act.[144] The court reasoned that it may have been in the websites' interests to imply the images were stolen in order to increase their appeal.[145] Thus, the website descriptions were not necessarily an admission that the photographs were stolen or illegal.[146] The court refused to "place the burden of determining whether photographs are actually illegal on a service provider."[147]

137. Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004) [hereinafter "*Perfect 10 I*"].

138. *See, e.g.*, *id.* ("[T]he DMCA requires that a copyright owner put the service provider on notice in a detailed manner but allows notice by means that comport with the prescribed format." (citing 17 U.S.C. § 512(c)(1))).

139. *Perfect 10 II*, 488 F.3d at 1108.

140. *Id.*

141. *Id.* at 1114.

142. *See id.*

143. *See* 17 U.S.C. § 512(c)(1)(A)(ii) (2006).

144. *Perfect 10 II*, 488 F.3d at 1114.

145. *Id.*

146. *Id.*

147. *Id.*

Most recently, the New York District Court addressed whether a service provider should be refused safe harbor protection if it has a mere general awareness of the presence of infringing material on the website.[148] In the case, plaintiff Viacom claimed its copyrighted works were uploaded to defendant YouTube's website.[149] Upon receiving a takedown notice from Viacom, YouTube removed the particular copyrighted item identified in the notice.[150] Viacom claimed YouTube's actions fell outside of the DMCA's safe harbor provisions because of "the replication, transmittal and display of [the] videos."[151]

Citing *Perfect 10 II*, the court held a general awareness that users may be prone to post infringing material is not sufficient to create an obligation for service providers to discover the infringing materials and remove them.[152] In so ruling, the court explained that § 512's knowledge requirement—that a service provider have actual knowledge the material is infringing—"describe[s] knowledge of specific and identifiable infringements of particular individual items."[153] This interpretation of the provision stems from the Act itself, which provides that application of safe harbor protection is not contingent on "'a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.'"[154] Such an application of the provision, the court noted, is also practical, as a service provider such as YouTube displays millions of user-generated items and, therefore, cannot be expected to inspect all content for illegal use.[155]

C. *Criticisms of the DMCA Safe Harbor Provisions*

Just as § 230 has received criticism for its broad immunity, the DMCA safe harbor provision is not without its critics. Much of that criticism has involved the alleged abuse of the takedown provision by copyright

148. Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010).

149. *Id.* at 518.

150. *Id.* at 519.

151. *See id.* at 526.

152. *See id.* at 523.

153. *Id.*

154. *Id.* at 524 (quoting 17 U.S.C. § 512(m)(1)).

155. *Id.* at 523. The court defended the effectiveness of the DMCA notification scheme by noting YouTube immediately removed nearly all of the infringing material after receiving a "mass take-down notice" from Viacom that addressed "some 100,000 videos." *Id.* at 524. Moreover, the court noted the volume of videos uploaded to YouTube was "over 24 hours of new video-viewing time . . . every minute." *Id.* at 518.

holders.[156] When a service provider receives notice from a copyright holder alleging copyright infringement, the service provider must decide between one of two actions: take the content down and enjoy the safe harbor provision, or refuse to take the content down and lose safe harbor protection, consequently facing full liability.[157] With such a large financial interest at stake, a service provider is more likely to err on the side of caution and simply remove the allegedly infringing material to avoid liability.[158] As a result of this very common occurrence, courts have not been afforded the opportunity to develop underlying service provider liability with respect to copyright infringement.[159]

There are two additional related critiques regarding the DMCA takedown procedure. First, in order to notify service providers of copyright infringement, copyright holders must either "monitor the entire Internet . . . or join a cartel of other copyright holders" to ensure copyrights are not being violated.[160] This can prove to be a difficult task, especially for smaller copyright holders that cannot afford constant monitoring or membership to a group.[161] Second, illegitimate takedown notices cease the spread of legal material.[162] Because service providers liberally remove allegedly copyrighted material and baseless or illegitimate notifications are inevitable, copyright holders who have material removed without their knowledge will be harmed.[163]

V. RECOMMENDATION FOR FIXING CDA § 230

Section 230 of the CDA, in its present state, has proven to be an unworkable piece of legislation, failing to accomplish Congress's intent in passing the provision and preventing many individuals from pursuing a remedy.[164] The Act was originally intended to allow websites to edit or

156. Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041, 1060 (2007) (footnotes omitted).

157. Craig W. Walker, Note, *Application of the DMCA Safe Harbor Provisions to Search Engines*, 9 VA. J.L. & TECH. 1, 14–15 (2004).

158. *See id.* at 14.

159. *Id.*

160. Jeffrey Cobia, Note, *The Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process*, 10 MINN. J.L. SCI. & TECH. 387, 397 (2009).

161. *Id.*

162. *Id.* at 398.

163. *See id.*

164. *See generally supra* Part III.B–D.

remove material without fear of liability for "providing" the information,[165] but the result has been a complete lack of policing by websites due to the broad immunity granted by courts.[166] Further, defamed persons with no ability to identify their defamers are left without recourse because the host website enjoys § 230 protection.[167] Although the recent decisions in *Roommates.com* and *Accusearch* represent an encouraging development, a website is still provided CDA immunity if it does not encourage infringing activity but has full knowledge of the activity.[168]

Although the DMCA has demonstrated an ISP liability system that holds websites with knowledge of infringing activity liable, an exact replica of that system would be impractical in the context of the CDA. First, the same issue would persist when websites, wanting to avoid liability, simply remove content without any consideration of the material's legitimacy.[169] Second, due to the incalculable amount of information posted to message boards, blogs, and media websites, a pure notice and takedown scheme would place an unreasonable amount of responsibility on ISPs.[170] Any individual who dislikes the information posted by another user could simply request the material be taken down. The ISP would subsequently have to decide if the content is indeed defamatory and whether it should be removed. This is a tremendous burden to place on ISPs and could result in the stunting of website development.[171]

For all the reasons listed above, a combination of the CDA and DMCA approaches should be adopted by Congress through a restructuring of § 230. First, the core holding of *Zeran*—that ISPs should not blindly be held liable for content posted to the website by third parties and that an

165. *See supra* notes 46–49 and accompanying text.

166. *See supra* Part III.B, D.

167. *See generally, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003) (failing to provide an adequate remedy to the plaintiff because the user who posted the defamatory and personal information was never identified, and the website owner was found not liable under § 230 immunity).

168. *See supra* Part III.C.

169. *See supra* Part III.B–D; *see also supra* notes 46–49 and accompanying text.

170. *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 518 (S.D.N.Y. 2010) ("[O]ver 24 hours of new video-viewing time is uploaded to the YouTube website every minute.").

171. *See* 47 U.S.C. § 230(b) (2006) ("[T]he policy [is] . . . 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 that presently exists for the Internet . . . .").

ISP is free to remove or edit content without becoming a distributor of that content—should stay intact.[172] Absent this interpretation, websites would be subjected to exponential liability.[173] Also, the holdings in *Roommates.com*[174] and *Accusearch*[175] should be perpetuated by courts. Any time an ISP encourages or requires third parties to post infringing material, that ISP should lose protection under § 230.[176] Allowing websites to encourage the posting of defamatory material does not further any of Congress's original justifications for the adoption of § 230.[177]

The similarities to the original § 230 should end there, however. The most important alteration Congress should make to § 230 is the implementation of an "opt-in requirement."[178] In order to enjoy the protections of § 230, an ISP must implement some variation of a user identification system.[179] Under such a system, a website must require all registered users to submit personal information, such as name, address, and e-mail to the ISP. Whether the submitted information is displayed to other users is left to the discretion of the individual. This elimination of anonymity would result in fewer instances of defamation and allow websites to avoid facing litigation every time defamatory material is posted. In the event that an individual feels he or she has been defamed, a request for personal information can be sent to the ISP. To prevent users from requesting personal information with no intention of pursuing litigation, the provision should include the threat of perjury for illegitimate requests.[180]

Although a pure notice and takedown system would be impracticable under the CDA, an ISP needs to be held liable in instances when the ISP

172. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

173. *See id.*

174. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1172 (9th Cir. 2008).

175. FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009).

176. *See id.*; *Roommates.com*, 521 F.3d at 1172.

177. *See* 47 U.S.C. § 230(b) (2006).

178. This should resemble the provision under the DMCA that requires a website to have in place a notification system and procedure for dealing with repeat offenders. *See* 17 U.S.C. § 512(i) (2010).

179. *Cf. id.* ("The limitations on liability established by this section shall apply to a service provider only if the service provider . . . has adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of [accounts for] repeat infringers . . . .").

180. The DMCA includes a similar provision, which places submitters of takedown notices under penalty of perjury. *See* 17 U.S.C. § 512(c)(3).

knows the material in question is defamatory. Therefore, when an ISP is aware of the posted information and reasonably should know of its defamatory nature, § 230 should not apply and the defamed should be able to recover from the ISP. Under such a provision, an ISP can essentially be held liable as a distributor of the material in question. This type of provision would avoid uncomfortable rulings similar to *Blumenthal v. Drudge*.[181] The ISP in *Blumenthal*, having contracted with and paid the author of the defamatory material, would likely lose § 230 protection under the proposed changes, as it reasonably should have known of the defamatory nature of content it paid to post.[182] Further, an ISP would certainly be stripped of CDA immunity if it encouraged users to post defamatory material; however, the opposite conclusion was implied by the court in *Blumenthal*, when § 230 immunity was extended.[183]

Such a provision may also help achieve one of Congress's original goals for adopting § 230: to encourage ISPs to self-regulate.[184] Knowing it could face liability if it is found to have acted unreasonably in the posting of defamatory content, an ISP may be more likely to monitor the website.[185] The Internet has progressed enough so that websites are able to absorb almost as much liability as a traditional distributor. A website should no longer be able to endorse and profit from known defamatory content while also enjoying absolute immunity from suit.

VI. CONCLUSION

Given that § 230 of the CDA has failed to encourage the self-regulation of websites by ISPs and has denied innumerable individuals the right to recovery in defamation suits, a restructuring of the CDA is vital to the enforcement of defamation law on the Internet. *Zeran* and its progeny have created an Internet where a website can be aware of and profit from defamatory content yet avoid liability.[186] The DMCA, with its pure notice and takedown scheme, demonstrates the necessity of holding an ISP liable when knowledge is demonstrable. Although an identical scheme appears

181. Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998); *see also supra* notes 69–73 and accompanying text.

182. *See Blumenthal*, 992 F. Supp. at 51.

183. *See id.* at 50.

184. *See* Zieglowsky, *supra* note 45.

185. *Cf.* Walker, *supra* note 157 (discussing the service provider's financial incentive to remove potentially infringing materials under the DMCA to avoid liability).

186. *See supra* Part III.B, D.

to be unworkable for the CDA, the requirement of a user identification system and the reapplication of distributor liability sufficiently narrows the immunity provided under § 230.

*Ryan Gerdes**

* Associate Attorney, Pillers & Richmond, De Witt, Iowa; J.D., Drake University Law School, 2011.