SYRACUSE SCIENCE AND TECHNOLOGY LAW REPORTER
VOLUME 19

Good Samaritan or Defamation Defender? Amending the Communications Decency Act to Correct the Misnomer of Section 230 . . . Without Expanding ISP Liability

Tara E. Lynch[1]

Fall 2008

INTRODUCTION

Falsely alleging that one has committed a crime of moral turpitude, carries a loathsome or contagious disease, or lacks integrity or ability in her trade or profession are widely recognized by lawyers and journalists as classic examples of per se defamation.[2] Imagine, for example, two female law students walking into your office, alleging that twenty-eight different people had published statements that they carried various venereal diseases, had effectively bought their way into law school despite poor LSAT scores, and had engaged in sexual relationships with the law school's deans. In theory, so long as these statements are false, this class of per se defamation suit seems at first blush easily won. That is until you ask who their alleged defamers are. They reply: "Pauliewalnuts," "neoprag," "Remember when I said I would kill you last? I Lied.," "The

[1] J.D. candidate, Syracuse University College of Law, 2009; Editor in Chief, *Syracuse Science and Technology Law Reporter*. The author would like to thank Professor Laura G. Lape for her support and helpful comments in advising this note. The author dedicates this note to her parents. The views expressed in this note are those of the author.

[2] *See* 50 AM. JUR. 2D *Libel and Slander* §§ 161-183; 200; 202-215 (2008).

Ayatollah of Rock-n-Rollah," "DRACULA," "Sleazy Z . . .". Welcome to defamation in the Internet age.

The preceding scenario is in fact the subject of the recently filed suit *Doe v. Ciolli*.[3] In their complaint, the two Jane Doe defendants – students at Yale Law School – allege that twenty-eight individuals, only identifiable by their online pseudonyms, tarnished their "character, intelligence, appearance and sexual lives" by posting a wide range of allegedly defamatory comments on the message boards of AutoAdmit.com.[4] As a result of the online smear, Doe I alleges that after sixteen interviews with law firms for summer employment she received no offers.[5] Anthony Ciolli, a law student and former director of AutoAdmit, was the only named defendant in the original complaint.[6] In the amended complaint[7], Ciolli was dropped from the suit, while eleven additional anonymous defendants were added.[8] While the AutoAdmit lawsuit has provided plenty of fodder for legal bloggers,[9] it also highlights an increasingly complex issue

[3] Complaint, Doe v. Ciolli, 307CV00909 CFD (D. Conn. June 11, 2007), *available at* http://wsj.com/public/resources/documents/aaComplaint.pdf.

[4] *Id.*

[5] *See* Amir Efrati, *Students File Suit Against Ex-AutoAdmit Director, Others*, WALL STREET JOURNAL ONLINE, June 12, 2007, http://blogs.wsj.com/law/2007/06/12/students-file-suit-against-autoadmit-director-others/; Ellen Nakashima, *Harsh Words Die Hard on the Web: Law Students Feel Lasting Effects of Anonymous Attacks*, WASH. POST, March 7, 2007, at A1.

[6] Ciolli had his job offer at a law firm revoked because of his involvement with the site. *See* Efrati, *supra* note 5.

[7] Amended Complaint, Doe I and Doe II v. John Does, 307CV00909 CFD (D. Conn. Nov. 8, 2007), *available at* http://online.wsj.com/public/resources/documents/ciollilawsuit.pdf.

[8] *See* Amit Efrati, *AutoAdmit Lawsuit Update: Ciolli Dropped*, WALL STREET JOURNAL ONLINE, Nov. 9, 2007, http://blogs.wsj.com/law/2007/11/09/autoadmit-lawsuit-update-ciolli-dropped/.

[9] For a compilation of news articles and blog posts about the AutoAdmit lawsuit, *see More on the AutoAdmit Lawsuit: An Update on Doe v. Ciolli*, http://www.abovethelaw.com/2007/06/an_update_on_doe_v_ciolli.php.

in online tort jurisprudence: How does one go beyond the pseudonym to obtain the identity of her alleged online defamer?[10]

As the Internet expands, so does the amount of legal commentary on this issue. By now, attorneys familiar with online tort issues are well aware that section 230(c) of the Communications Decency Act (hereinafter "CDA") – commonly known as the "Good Samaritan" provision – insulates Internet Service Providers (hereinafter "ISPs") from civil liability for carrying defamatory or otherwise tortious material on their services.[11] Therefore, in order for a defamed plaintiff to have her day in court, she must get a subpoena ordering the ISP to reveal the identity of her anonymous online defamer. In light of First Amendment concerns, courts to date have refused to establish a uniform test to be applied when deciding whether a defamation claim has enough merit to justify a subpoena to the ISP. This, foreseeably, has caused problems in litigation. In the best-case scenario, defamed plaintiffs seek subpoenas blindly, unaware of which standard the court will apply. In the worst-case scenario, plaintiffs are left with no legal recourse at all when courts struggling to determine a standard fail to act expeditiously, since many ISPs only store the IP addresses used to identify John Doe defamers for a limited period.[12]

---

[10] Later, Doe I managed to identify one alleged defamer known as AK47 by issuing a subpoena to AT&T. In *Doe I v. Individuals*, 561 F. Supp. 2d 249 (D. Conn. 2008), AK47 moved the court to quash the subpoena seeking his identity and moved for permission to proceed with the litigation anonymously. Applying the "sufficient evidence" approach, discussed *infra* at notes 116-130, the court denied the motion to quash, and denied the motion to proceed anonymously. Later, the Does filed an amended complaint, also naming Matthew C. Ryan, previously known as ":D" as a defendant. *See* Citizen Media Law Project, *Doe v. Ciolli*, http://www.citmedialaw.org/threats/doe-v-ciolli (last visited Aug. 14, 2008).

[11] 42 U.S.C. § 230(c) (2006).

[12] *See infra* note 81.

This note argues that section 230(c) of the CDA should be amended by codifying the summary judgment standard for ISPs announced in *Doe v. Cahill*[13] by the Delaware Supreme Court. Indeed, once an ISP subpoena standard has been codified – as the Digital Millennium Copyright Act (hereinafter "DMCA") has done in section 512(h) for copyright infringement actions – courts, plaintiffs, and ISPs will be able to better predict when a John Doe's identity is discoverable. Moreover, codifying a subpoena standard, rather than expanding the liability of ISPs, will make the "Good Samaritan" provision what it purports it to be: protective of First Amendment interests and ISPs, yet still accommodating to meritorious defamation claims. As currently enacted, the latter simply is not true.

Part I of this note will summarize the right to free speech under the First Amendment, the tort of defamation, and how the right to speak anonymously has uniquely affected Internet-based defamation claims. Part II will examine the pertinent CDA provision, section 230, and its legislative history. Part III will provide an overview of recent John Doe defamation suits and the tests courts have applied in determining whether to subpoena ISPs for the identities of John Doe defendants. Part III of this note will then examine and critique additional solutions to this problem proposed by commentators. In Part IV, I will argue that section 230 of the CDA should be amended by codifying the summary judgment standard announced in *Cahill*. Part IV will then suggest statutory language for the proposed section 230 amendment, borrowing in part from the subpoena language enacted by Congress in section 512(h) of the DMCA. Part V will conclude this note.

I. DEFAMATION IN THE (INTERNET) AGE OF UNINNOCENCE

a. Speaking Freely and Anonymously Online

[13] Doe v. Cahill, 884 A.2d 451, 462-65 (Del. 2005).

The First Amendment to the Constitution provides that "Congress shall make no law . . . abridging the freedom of speech . . ."[14] The right to speak freely, as established by the Free Speech clause, is one of the most revered and fiercely protected rights enjoyed by American citizens.[15] It is no surprise then that the right to speak freely has been recognized as extending to anonymous speech, speech on the Internet, and in turn, anonymous speech on the Internet.

The United States Supreme Court has recognized that the Free Speech Clause protects anonymous speech.[16] In *Talley v. California*, for example, the Court invalidated a Los Angeles ordinance prohibiting all anonymous leafleting.[17] Similarly, in *McIntyre v. Ohio Elections Commission*, the plaintiff challenged an Ohio statute that prohibited the distribution of anonymous campaign literature.[18] The Court found the statute unconstitutional, noting, "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[19]

The Court has also recognized that the protections of the First Amendment extend to the Internet.[20] In *Reno v. ACLU*, for example, the court struck down as unconstitutional two

---

[14] U.S. CONST. amend. I.

[15] The First Amendment is made applicable to the states by the Fourteenth Amendment. U.S. CONST. amend. XIV.

[16] *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 200 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).

[17] *Talley*, 362 U.S. at 66. In so holding, the court noted that "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." *Id.* at 64.

[18] *McIntyre*, 514 U.S. at 338.

[19] *Id.* at 342.

[20] Reno v. ACLU, 521 U.S. 844 (1997).

provisions of the CDA that sought to protect minors from harmful material on the Internet.[21] The basis of the Court's decisions was that the provisions at issue abridged the "freedom of speech" protected by the First Amendment, even on the Internet.[22]

b. The Tort of Defamation

While the protection afforded speech by the First Amendment is broad, it is not absolute.[23] Indeed, "[t]here are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem."[24] One such class of speech which is not protected by the First Amendment is defamatory speech.[25]

Public policy recognizes that individuals have the right to enjoy their reputation, free from false attacks that tend to diminish their reputation in the eyes of the community.[26] When this right is violated, a plaintiff may bring an action for defamation against the speaker of the false attack to vindicate the damage to his or her reputation.[27] The law of defamation recognizes the twin torts of libel, which is brought when the defamatory statement is published in a "fixed

---

[21] At issue in *Reno* were 47 U.S.C. § 223(a)(1)(B)(ii), which criminalized the "knowing" transmission of "obscene or indecent" material to persons under age 18, and 47 U.S.C. § 223(a), which criminalized the knowing sending or displaying of such materials to persons under age 18; *see Reno*, 521 U.S. at 849.

[22] *Reno*, 521 U.S. at 849.

[23] *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 571 (1942).

[24] *Chaplinsky*, 315 U.S. at 571-72. In *Chaplinksy*, the Supreme Court held that the New Hampshire statute under which Chaplinsky was charged – which forbade "address[ing] any offensive, divisive or annoying word to any other person who is lawfully in any street or other public place" – did not violate the First Amendment to the U.S. Constitution. *Id.* at 569. The Court found that the "fighting words" at issue in the case – as well as speech that is profane, lewd, obscene, or libelous – is not protectable under the First Amendment because "such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality." *Id.* at 572.

[25] *Id.* at 572.

[26] 50 AM. JUR. 2D *Libel and Slander* § 2 (2008).

[27] *Id.*

medium," and slander, which is brought when the defamatory statement is spoken.[28] Because defamation is a state law claim,[29] the elements can vary slightly among jurisdictions. However, a claim for defamation usually requires: (1) a false and defamatory (purported) statement of fact; (2) of and concerning the plaintiff; (3) unprivileged publication; (4) harm to the plaintiff; and (5) fault amounting to at least negligence[30] on the part of the publisher.[31] The burden to prove each element rests on the plaintiff.[32]

The pre-trial stages of a defamation lawsuit traditionally follow the same course as other civil litigation: the plaintiff files a complaint, the defendant is served and responds, and discovery ensues. When the defendant-defamer is clearly identifiable, these steps remain the same, and the complaint is served to the defendant. Even when the defamer is anonymous in contexts other than the Internet, the process of litigation is largely unchanged. For example, if a newspaper publishes an article with an anonymous statement of and concerning the plaintiff, and the plaintiff wishes to bring a defamation claim, he or she is free to serve the newspaper defendant/publisher of the defamatory content. The situation becomes more complicated,

---

[28] *Id.* §§ 1, 9; BLACK'S LAW DICTIONARY 934, 1421 (8th ed. 2004). Because this note addresses defamatory statements published online, the specific cause of action addressed is libel. Nonetheless, I will reference defamation generally in this note.

[29] 50 AM. JUR. 2D *Libel and Slander* §15 (2008).

[30] A public official or public figure plaintiff must prove that the defendant published the defamatory statement with actual malice, that is, with knowledge that the statement was false or with reckless disregard for the truth. New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964). A private plaintiff, in contrast, must show fault amounting to at least negligence. Gertz v. Welch, 418 U.S. 323, 350 (1974). While the distinction between public and private plaintiffs is important in a defamation case, it does not come into play for purposes of the *Cahill* summary judgment subpoena standard, or the amendment proposed in this note, because neither requires a showing of fault on the part of the defendant before a subpoena is issued. *See infra* notes 146-48.

[31] *See generally* 50 AM. JUR. 2D *Libel and Slander* § 21; RESTATEMENT (SECOND) OF TORTS § 558 (1977) (listing the elements of defamation as: "(a) a false and defamatory statement concerning another; (b) an unprivileged publication to a third party; (c) fault amounting at least to 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").

[32] 50 AM. JUR. 2D *Libel and Slander* § 478 (2008).

however, when the plaintiff's defamer hides behind the veil of an online pseudonym, because unlike newspapers, ISPs are immune from civil liability.

II. THE COMMUNICATIONS DECENCY ACT[33]

In 1995, there were 16 million Internet users, or 0.4% of the world's population.[34] It was against this backdrop that Senator J.J. Exon (D-NE), concerned that the available communications laws were woefully out of date, introduced the legislation that became the CDA.[35] The primary purpose of the CDA, as originally proposed, was to revise the then-existing telecommunications laws to encompass the growth of the World Wide Web.[36] Specifically, the legislation was intended to impose liability on those who used telecommunications devices – namely the fledgling Internet – to distribute obscene or indecent materials to minors.[37]

a. Section 230

The original Senate version of the CDA included only the prohibitions against and penalties for distributing obscene material over the Internet to minors, and did not include section 230, which was added by conference amendment in the House of Representatives. The amendment, proposed by Representatives Chris Cox (R-CA) and Ron Wyden (D-CA), came as a

---

[33] For a thorough examination of the legislative history of the CDA, *see* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, *available at* http://www.law.indiana.edu/fclj/pubs/v49/no1/cannon.html (last visited Oct. 17, 2008).

[34] *Internet Growth Statistics*, http://www.Internetworldstats.com/emarketing.htm (last visited Oct. 17, 2008).

[35] 141 CONG. REC. S8087-04 (daily ed. June 9, 1995) (statement of Sen. Exon).

[36] *Id.*; As Senator Exon stated: "T[]he information superhighway should not become a red light district. This legislation will keep that from happening and extend the standards of decency which have protected telephone users to new telecommunications devices." 141 CONG. REC. S1953 (daily ed. Feb. 1, 1995) (statement of Sen. Exon).

[37] *Id.* The CDA was Congress' first attempt to try to regulate the availability of pornography to minors on the Internet. However, many of the CDA provisions enacted for that very purpose were later found to be unconstitutional violations of the First Amendment in *Reno v. ACLU*. *See Reno*, 521 U.S. 844, discussed *supra* at fns. 20-27.

direct response to the New York decisions *Cubby, Inc. v. CompuServe, Inc.*[38] and *Stratton Oakmont, Inc. v. Prodigy Services*.[39] Specifically, the amendment statutorily overruled the then-recent *Stratton Oakmont* decision, which had held an ISP could be held liable for defamatory material posted by its users.[40]

One of the earliest decisions to illustrate the risks to which ISPs are exposed was the *Cubby* case. In *Cubby*, the plaintiffs developed "Skuttlebut," a database designed to develop and distribute news and gossip.[41] Defendant CompuServe, an ISP, provided its customers with the CompuServe Information Service, a compilation of news services and special forums which ISP members paid a fee to access.[42] One feature of the CompuServe Information Service was the Journalism Forum, which featured "Rumorville USA."[43] Rumorville USA was a daily online newsletter compiled by outside journalists.[44] CompuServe hosted the online newsletter, but had no contractual or employment relationship with the journalists who created it.[45]

The plaintiff sued CompuServe and other defendants for libel, claiming that Rumorville USA published false and defamatory statements related to Skuttlebut, and claiming that CompuServe should be held liable since it carried Rumorville USA on its Journalism Forum.[46]

---

[38] Cubby, Inc. v. Compuserve, Inc., 776 F.Supp. 135 (S.D.N.Y. 1991).

[39] Stratton Oakmont, Inc. v. Prodigy Service Co., 1995 WL 323710 (N.Y. Sup. May 25, 1995).

[40] *See infra*, notes 41-49; *see also* 141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) for representatives Cox's and Goodlatte's criticisms of the *Stratton Oakmont* decision.

[41] *Cubby, Inc.,* 776 F.Supp. at 138.

[42] *Id.* at 137.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Cubby, Inc.,* 776 F.Supp. at 138.

CompuServe argued that because it was a distributor rather than of a publisher of Rumorville USA, it could only be held liable if it knew or had reason to know of the defamatory comments.[47] The court agreed, finding that CompuServe was only a distributor of Rumorville USA, because it exercised no editorial control over its content.[48] Therefore, because the plaintiffs failed to allege facts showing that CompuServe had knowledge of the alleged defamatory content, the court refused to hold CompuServe liable on the plaintiff's libel claim.[49]

The opposite result was reached in the *Stratton Oakmont* decision. In that case, the plaintiff brought a defamation claim against Prodigy, an ISP, for allegedly posting defamatory content on Prodigy's "Money Talks" message board.[50] Stratton Oakmont, a securities investment firm, identified as defamatory comments that had been posted anonymously on the message board.[51] The comments asserted that the company had engaged in criminally fraudulent activities in its handling of a client's initial public offering.[52] In addressing Prodigy's liability, the court noted that Prodigy had "held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper."[53]

---

[47] *Cubby, Inc*., 776 F.Supp. at 138. The *Cubby* court explained: "Ordinarily, 'one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.' Cianci v. New Times Publishing Co., 639 F.2d 54, 61 (2d Cir. 1980) . . . With respect to entities such as news vendors, book stores, and libraries, however, 'New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.' Lerman v. Chuckleberry Publishing, Inc., 521 F.Supp. 228, 235 (S.D.N.Y.1981); *accord* Macaluso v. Mondadori Publishing Co., 527 F.Supp. 1017, 1019 (E.D.N.Y. 1981)." *Cubby, Inc.,* 776 F.Supp. at 139.

[48] *Cubby, Inc*., 776 F.Supp. at 140.

[49] *Id.* at 141.

[50] *Stratton Oakmont, Inc.*, 1995 WL 323710, at *1.

[51] *Id.*

[52] *Id.*

[53] *Id.* at *2.

Therefore, the court found that Prodigy was a publisher rather than a distributor of the allegedly defamatory material, and as such could be held liable on the plaintiff's defamation claim.[54]

Section 230 was proposed as a direct reaction to the *Stratton Oakmont* decision. Specifically, Representatives Cox and Wyden were concerned that ISPs would be unwilling to help them enforce the original purpose of the CDA – keeping pornography out of the hands of minors – if doing so would expose them to civil liability.[55] As Representative Cox noted, "[w]e want to encourage people like Prodigy, like CompuServe, like America Online, like the new Microsoft network, to do everything possible for us."[56] The stated purpose of section 230 was two-fold: (1) to "protect computer Good Samaritans, online service providers, anyone who provides a front end to the Internet . . . who takes steps to screen indecency and offensive material for their customers;" and (2) to "establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet."[57] Representatives Cox and Wyden's amendment to the CDA was ultimately accepted by Conference agreement, where it was noted "[o]ne of the specific purposes of this section is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."[58] Thus, Congress saw to fruition its intended

---

[54] *Id.* at *5.

[55] "The New York Supreme Court, held that Prodigy, CompuServe's competitor, could be held liable in a $200 million defamation case because someone had posted on one of their bulletin boards, a financial bulletin board, some remarks that apparently were untrue about an investment bank, that the investment bank would go out of business and was run by crooks . . . Mr. Chairman, that is backward." 141 CONG. REC. H8460-01, H8469-70 (daily ed. Aug. 4, 1995) (statement of Sen. Cox).

[56] 141 CONG. REC. H8460-01, H8469-70 (daily ed. Aug. 4, 1995) (statement of Sen. Cox).

[57] *Id.*

[58] H.R. CONF. REP. No. 104-458, at 194 (1996) (Conf. Rep.).

purpose – keeping obscenity away from minors on the Internet – and ISPs were relieved of the civil liability they feared in the wake of *Stratton Oakmont*.

As finally enacted, section 230(c) – the specific subsection that insulates ISPs from civil liability stemming from content created by third parties – provides:

> (c) Protection for "good samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> 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.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of--
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[59]

As defined in subsection (f),

> The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.[60]

---

[59] 47 U.S.C. § 230(c) (2008).

[60] 47 U.S.C. § 230(f)(2).

It is generally recognized that an "interactive computer service," as defined, includes what are more commonly referred to as ISPs. However, section 230(c) did not insulate ISPs from all causes of action; section 230(e) preserved ISP liability for criminal law,[61] intellectual property law,[62] communications privacy laws,[63] and consistent state law.[64]

It soon became clear that state tort law – including defamation actions – were in that class of inconsistent state laws that were subject to section 230(c)'s broad immunity provisions. The effect of section 230 of the CDA was to insulate ISPs from almost all defamation causes of action. Of course, it was impossible for Congress to know that at the time of section 230's enactment how far reaching its impact would be. Indeed, after the enactment of the CDA, the Internet continued to expand in ways perhaps unanticipated by Congress. By December 1996, less than a year after the CDA was enacted, there were 36 million Internet users.[65] A year later, the number of Internet users had doubled to 70 million users.[66] Today, there are almost 1.3 billion Internet users worldwide.[67] As the number of Internet users grew, so did the amount of defamatory material online.

b. The *Zeran v. America Online* Decision

[61] 47 U.S.C. § 230(e)(1).

[62] 47 U.S.C. § 230(e)(2).

[63] 47 U.S.C. § 230(e)(4).

[64] 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

[65] *Internet Growth Statistics*, *supra* note 34.

[66] *Id.*

[67] *Id.*

It was not until *Zeran v. America Online, Inc.,* that it became clear exactly how insulated ISPs were as a result of section 230(c).[68] The *Zeran* decision, decided two years after the CDA's enactment, was the first decision to apply section 230 in a defamation case against an ISP. An unidentified person had posted a message on an AOL message board advertising the sale of t-shirts featuring offensive slogans related to the Oklahoma City bombings.[69] Interested buyers were told to contact "Ken" at plaintiff Ken Zeran's home phone number.[70] As a result, Zeran received a high volume of angry calls, including death threats.[71] Zeran contacted AOL with his predicament, and an AOL employee agreed to remove the posting.[72] The next day, however, another message advertising the shirts appeared, again directing interested buyers to contact the plaintiff.[73]

The number of angry, threatening calls the plaintiff received intensified, and the unidentified poster continued to post messages on AOL's bulletin board over the next four days.[74] Zeran contacted AOL several times, and was told that the posting user's account would be closed.[75] In the meantime, an Oklahoma radio station which received wind of the posts encouraged listeners to call the plaintiff.[76] As a result, the plaintiff received numerous death

---

[68] *See* Zeran v. Am. Online, Inc.*,* 129 F.3d 327 (4th Cir. 1997).

[69] *Zeran*, 129 F.3d at 329.

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Zeran*, 129 F.3d at 329.

[75] *Id.*

[76] *Id.*

threats.[77] In desperation, Zeran reported the incident to the FBI in Seattle, and local police had to guard his home.[78]

Ultimately, after an Oklahoma City newspaper published a story exposing the hoax, the number of calls plaintiff received began to subside.[79] The *Zeran* case confirmed that online defamation – with its ability to spread across the country with the click of a mouse – was more than just a matter of hurt feelings, but a serious threat to its victims.

Zeran sued AOL, arguing that the ISP unreasonably delayed in removing the defamatory materials posted by the John Doe.[80] Zeran, however, did not sue the John Doe that posted the messages, since "AOL made it impossible to identify the original party by failing to maintain adequate records of its users."[81] The district court granted judgment for AOL, finding that section 230 barred Zeran's claims.[82] On appeal, Zeran again argued that section 230 left intact civil liability for ISPs who had notice of defamatory material posted on their services.[83] In essence, Zeran attempted to revive the distributor-publisher distinction discussed in the *Cubby*[84] and *Stratton Oakmont*[85] cases, and argued that although section 230 had insulted ISPs from publisher liability, distributor liability was left intact by the CDA.[86]

---

[77] *Id.*

[78] *Id.*

[79] *Zeran*, 129 F.3d at 329.

[80] *Id.* at 328.

[81] *Id.* at 329-30.

[82] *Id.* at 328.

[83] *Id.*

[84] *Cubby, Inc.,* 776 F.Supp. at 139-42.

[85] *See Stratton Oakmont, Inc.,* 1995 WL 323710, at *3-5.

[86] *Zeran,*129 F.3d at 330.

The Court of Appeals disagreed.

> [Section] 230 creates a federal immunity to any cause of action that would make services providers liable for information originating with a third-party user of the service . . . Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred.[87]

In so holding, the court looked to Congress' intent in enacting section 230:

> Congress enacted § 230 to remove the disincentives to self regulation created by the *Stratton Oakmont* decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). In line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.[88]

Addressing Zeran's distributor liability theory, the court noted that "this theory of liability is merely a subset, or species, of publisher liability, and is therefore also foreclosed by § 230."[89] Indeed, the court explained that while AOL is legally considered a publisher, in regards to defamation law, the distinction between distributors and publishers is of little import.[90] For the purposes of defamation law, everyone who takes part in the publication of the defamatory

---

[87] *Zeran,*129 F.3d at 330.

[88] *Id.* at 331.

[89] *Id.* at 332.

[90] *Id.*

statement is charged with publication, including distributors.[91] The distinction, thus, is intended only to determine *when* liability attaches.[92]

III. STANDARDS OF LIABILITY

In the wake of *Zeran*, it was clear that section 230(c) completely insulated ISPs from liability for content created by third-party users of their services.[93] For plaintiffs who could identify their online defamer, the loss was simply monetary. While unable to go after the deep pockets of the ISPs, such plaintiffs are still free to sue their known online defamers, and many do.[94]

However, difficulties arise for plaintiffs when their alleged defamer is a John Doe. The Supreme Court has recognized the right of plaintiffs to sue unknown defendants,[95] however, technical issues do arise. Because defamation is a state law claim, it is generally brought in state court,[96] so the procedure for obtaining a John Doe defendant's identity can vary slightly from

---

[91] *Id.* at 331-32.

[92] *Id.* at 332, *citing* W. Page Keeton et al., *Prosser and Keeton on the Law of Torts*, §113 (5th ed. 1984).

[93] *Zeran,*129 F.3d at 330.

[94] *See, e.g.,* Goldhaber v. Kohlenberg, 928 A.2d 948 (N.J. Super. Ct. App. Div. 2007) (where a punitive damage award of $1,000,000 to plaintiffs who were defamed by defendant online was remanded to determine compliance with the Punitive Damages Act); Overstock.com, Inc. v Gradient Analytics, 61 Cal. Rpt. 3d 29 (Cal. Ct. App. 2007) (finding that plaintiff, an online retailer, had stated a cause of action for defamation where the defendant analytics company published false reports about the plaintiff's accounting in online analytic reports to satisfy its hedge fund customers); Gulrajaney v. Petricha, 885 A.2d 496 (N.J. Super. Ct. App. Div. 2005) (plaintiff, a candidate for a seat on a condominium association board, failed in defamation action against defendants who posted defamatory statements to the condominium message board because plaintiff, a limited public figure, failed to prove actual malice).

[95] *See* Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388, 388 (1971).

[96] Of course, defamation claims can be brought in or removed to federal court if diversity exists between the parties. However, it is impossible to know if diversity between the parties exists unless the identity of the John Doe defendant is discovered. Because this note deals exclusively with the standards to be applied by state courts in issuing subpoenas compelling ISP to reveal the identity of John Does, I do not address the other jurisdictional challenges of bringing a John Doe suit in federal court. For a discussion of some of those challenges, *see* Megan Sunkel, *And the I(SP)S have it . . . But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the identity of Anonymous Internet Users In Claims Of Online Defamation*, 81 N.C. L. REV. 1189, 1198-1207 (2003).

state to state. Under the Federal Rules of Civil Procedure, and in those states adopting those rules, "[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order."[97] Therefore, the only way a plaintiff can discover the identity of a John Doe defendant is to file an ex-parte motion seeking a subpoena compelling the ISP to disclose the John Doe's identity.[98] Moreover, a court order is necessary because federal law prohibits a cable ISP from disclosing the identity of a subscriber unless it does so pursuant to court order and the subscriber is notified.[99]

ISPs are generally able to ascertain the identities of John Doe defendants by tracing their "Internet protocol address" (hereinafter "IP address").[100] An IP address is a unique, electronic number which specifically identifies a device (often a computer) connected to the Internet.[101] Often, ISPs own particular IP addresses, which are then assigned to their individual subscribers.[102] Therefore, armed with an IP address, and the date and time a posting was made, an ISP can identify almost any of its subscribers.[103]

---

[97] FED. R. CIV. P. 26(d)(1).

[98] *See e.g.,* McMann v. Doe, 460 F.Supp.2d 259, 262-63 (D. Mass 2006).

[99] 47 U.S.C. § 551(c)(2)(B).

[100] *Cahill*, 884 A.2d at 454-55.

[101] *Id.*

[102] *Id.*

[103] *Id.* at 455.

Of course, once an ISP is compelled by court order to reveal the identity of a John Doe defendant, it must comply.[104] However, what standards state courts will apply in deciding whether to compel disclosure is less clear.

A. Confusion in the Courts: "Good Faith" to Summary Judgment

Since *Zeran*, state courts have applied a variety of standards in deciding whether to subpoena ISPs for this purpose, from a plaintiff-friendly "good faith" standard to speech-protective summary judgment approach.[105]

1. Protecting Plaintiffs: The *America Online* "Good Faith" Standard

Arguably, the first defamation case to address the issue of whether an ISP should be compelled to disclose a John Doe defendant's identity[106] was *In re Subpoena Duces Tecum to America Online, Inc.*[107] In that case, America Online ("AOL") sought to quash a subpoena compelling it to disclose the identities of five of its subscribers.[108] The plaintiff company had obtained a subpoena from the Virginia court – although its defamation action against the John Does was pending in Indiana – compelling AOL to reveal the defendants' identities.[109] AOL, however, refused to comply, arguing that the subpoena unduly burdened its subscribers' First

---

[104] 47 U.S.C. § 551(c)(2)(B) (requiring that the ISP also notify the John Doe that his identity is being sought).

[105] For another recitation of the standards courts have applied, *see* Charles B. Vincent, *Cybersmear II: Blogging and the Corporate Rematch Against John Doe, Version 2.006*, 31 DEL. J. CORP. L. 987, 996-1008 (2006).

[106] One earlier case – Columbia Ins. Co. v. Seescandy.com, 185 F.R.D.573 (N.D. Cal. 1999) – addressed the issue of whether a plaintiff should be allowed to conduct limited discovery to obtain the anonymous defendant's identity so that service could be properly affected. The claim in that case, however, was trademark infringement, so the same First Amendment concerns that arise in defamation claims were not implicated.

[107] In re Subpoena Duces Tecum to Am. Online, Inc., No. 405702000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000)., *rev'd on other grounds* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001).

[108] *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372 at *1.

[109] *Id.*

Amendment right to speak anonymously.[110] The court acknowledged that the right to speak anonymously on the Internet could be implied from the Supreme Court's decisions in *McIntyre* and *Reno*.[111] However, it also noted that the right to speak anonymously in any medium was not absolute, and that "[t]hose who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights."[112]

In balancing the First Amendment interests of the John Does with the plaintiff's interest in redress, the court determined that a non-party ISP should be compelled to disclose the identities of its subscribers:

> (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim.[113]

In choosing a "good faith" standard, the court decided that the compelling state interest in protecting plaintiffs from potentially damaging statements on the Internet outweighed the limited intrusion on an anonymous poster's First Amendment rights.[114] Ultimately, based on the

---

[110] *Id.* at *2. In its brief, AOL acknowledged that it had complied with hundreds of subpoenas issued by Virginia courts when "(1) that the party seeking the information has pled with specificity a prima facie claim that it is the victim of particular, specified tortious conduct and (2) that the subpoenaed identity information was centrally needed to advance the claim." *Id.* at *1 n. 3. AOL suggested that the court adopt this two-prong test in determining whether a court should enforce such subpoenas; the plaintiff argued that the court should in no way consider the merits of the claim. *Id.* at *7.

[111] *In re Subpoena Duces Tecum to Am. Online, Inc.*, 2000 WL 1210372 at *6.

[112] *Id.*

[113] *Id.* at *8.

[114] *Id.*

pleadings and the chatroom logs, the court determined that the plaintiff had satisfied this "good faith" standard, and denied AOL's motion to quash the subpoena.[115]

2. The "Sufficient Evidence" Approach

The plaintiff-friendly approach announced by the Virginia court was limited geographically. Indeed, just a year after the decision in *America Online*, the New Jersey appellate court denounced the "good faith" approach in favor of a standard that was more speech protective.[116] In *Dendrite International v. John Doe No. 3*, the plaintiff corporation attempted to discover the identity of John Doe No. 3, who under the pseudonym "xxplrr" had allegedly posted defamatory comments about the company on Yahoo's Dendrite bulletin board.[117] Dendrite International ("Dendrite") claimed that the "xxplrr" postings had damaging effects on its hiring practices and on the company's stock value.[118] The trial court, however, had denied Dendrite's request for expedited discovery of the John Doe defendant's identity.[119] Specifically, the lower court found that Dendrite had failed to establish a prima facie claim for defamation, since the company failed to show that harm resulted from the "xxplrr" messages.[120] This appeal followed.

In affirming the trial court's denial of Dendrite's request, the court set out a four-part "sufficient evidence" approach for determining when an ISP would be compelled to disclose a

---

[115] *Id.*

[116] Dendrite Int'l v. John Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001). In *Dendrite*, the court noted: "The Virginia case supports the notion that when evaluating a plaintiff's request to compel an ISP to disclose the identity of a John Doe subscriber, courts may depart from traditionally-applied legal standards in analyzing the appropriateness of such disclosure in light of the First Amendment implications." *Dendrite*, 775 A.2d at 771.

[117] *Id.* at 760.

[118] *Id.* at 772.

[119] *Id.* at 760. In total, the *Dendrite* case involved four John Doe plaintiffs. The trial judge granted Dendrite's motion for expedited discovery as to John Does Number 1 and 2, but denied the motion as to John Does Number 3 and 4. Only the motion as to John Doe Number 3 was at issue in this appeal. *Id.* at 764.

[120] *Id.* at 764.

John Doe subscriber's identity.[121] First, the court required that the plaintiff attempt to notify the John Doe that he was the subject of a subpoena compelling his identity, and give the anonymous defendant sufficient time to file an opposition to the discovery request.[122] The court stated that such notification could be effected by, for example, posting notice of the subpoena on the appropriate message board.[123] Second, the plaintiff must "identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech."[124] Third, the court must be satisfied that the plaintiff's pleadings would survive a motion to dismiss, *and* that the plaintiff had "produce[d] sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant."[125] Lastly, the court required a balancing of the plaintiff's prima facie case and the necessity of disclosure of the defendant's identity against the John Doe's First Amendment interest in anonymous speech.[126] Thus, even if the plaintiff presents sufficient evidence of each prima facie element of his defamation claim, the court will not necessarily compel the ISP to reveal John Doe's identity.[127] Although the court announced the new standard, it did not have a chance to apply it fully.[128] Indeed, the appellate court agreed with the trial court that Dendrite had failed to show that John Doe No. 3's posting had caused the

---

[121] Dendrite, 775 A.2d at 760.

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Dendrite*, 775 A.2d at 760-61.

[127] *Id.*

[128] *See id.* at 772.

company harm, and thus refused to compel discovery of John Doe's identity.[129] While no other cases appear to have applied the "good faith" approach announced in *Zeran*, *Dendrite*'s "sufficient evidence" standard has been cited favorably by other New Jersey courts.[130]

3. The "Summary Judgment" Standard

Doe v. Cahill was the first case in which a state Supreme Court had occasion to address the standard that trial courts should apply in deciding whether to compel ISPs to disclose the identities of alleged John Doe defamers.[131] Under the alias "Proud Citizen," the defendant[132] posted two statements on a local "Issues Blog" concerning town councilman Patrick Cahill.[133] The posts stated that Cahill was a poor leader and suffered from mental illness.[134] In turn, the plaintiff brought suit for defamation and invasion of privacy. After obtaining leave from the lower court to conduct a pre-service deposition of the blog owner, the plaintiff discovered the IP address of the defendant, which was owned by the Comcast Corporation.[135] The plaintiff then obtained a court order requiring Comcast to disclose the defendant's identity.[136] As required by

---

[129] *Id.* In fact, the court noted that although Dendrite's stock value had decreased immediately following John Doe No. 3's posting, the stock value ultimately increased. During the week that the postings were made, Dendrite's stock had a net increase in value of 3 and 5/8 points. *Id.*

[130] *See* Immunomedics, Inc. v. Doe, 775 A.2d 773 (N.J. Super. Ct. App. Div. 2001) (decided the same day as *Dendrite*); Donato v. Moldow, 865 A.2d 711 (N.J. Super. Ct. App. Div. 2005); Greenbaum v. Google, Inc., 875 N.Y.S.2d 695 (N.Y. Sup. Ct. 2007).

[131] *Cahill*, 884 A.2d at 457.

[132] Cahill's initial claim named four John Doe defendants; only one John Doe defendant was at issue on this appeal. *See id.* at 454.

[133] *Id.*

[134] *Id.* The first of the two posts stated that Cahill was "a divisive impediment to any kind of cooperative movement," "a prime example of failed leadership," and alleged that he suffered from "obvious mental deterioration." A second post stated: "*Gahill* [sic] *is as paranoid* as everyone in town thinks he is." *Id.*

[135] *Id.*

[136] *Cahill*, 884 A.2d at 455.

Federal Statute,[137] Comcast notified the defendant that his identity was being sought;[138] the defendant immediately filed an "Emergency Motion for a Protective Order" to prevent his identity from being disclosed.[139] After adopting a "good faith" standard for determining when the plaintiff could compel disclosure of a John Doe defendant's identity, the trial court denied Doe's motion for a protective order and ordered disclosure of his identity.[140]

On appeal, the Delaware Supreme Court rejected the "good faith" standard announced in *Zeran*[141] and adopted by the trial court, finding it "too easily satisfied to protect sufficiently a defendant's right to speak anonymously."[142] The court also found that a motion to dismiss standard – like that applied in *Ramunno v. Cawley*[143] – although "more stringent," fell short of the protection required by the First Amendment.[144] Ultimately, the court decided to adopt a modified version of the *Dendrite* "sufficient evidence" standard.[145] Specifically, the court retained the first and third parts of the *Dendrite* test, while rejecting the second and fourth prongs of the test.[146] In doing so, the court noted that the second prong – requiring the plaintiff to set

---

[137] *See* 47 U.S.C. §551(c)(2).

[138] *Cahill*, 884 A.2d at 455.

[139] *Id.*

[140] *Id.*

[141] *See Zeran*,, 129 F.3d 327.

[142] *Cahill*, 884 A.2d at 458.

[143] Ramunno v. Cawley, 705 A.2d 1029 (Del. 1998). Specifically, the *Cahill* court noted that because Delaware is a notice-pleading jurisdiction, a motion to dismiss standard would only require a plaintiff to give "general notice of the claim asserted" to defeat a motion to dismiss. *Cahill*, 884 A.2d at 458. This standard, of course, is far lower than the requirement to prove each element of the prima facie case as announced in *Dendrite* and *Cahill*.

[144] *Cahill*, 884 A.2d at 458.

[145] *Id.* at 461.

[146] *Id.*

forth the exact defamatory statements – and the fourth prong – requiring a balancing of interests – were already considered in the third prong's "summary judgment" inquiry.[147] Thus, under the *Cahill* summary judgment standard, a plaintiff seeking to compel disclosure of an anonymous plaintiff's identity must: (1) "undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure," and (2) satisfy the summary judgment standard – that is, present evidence of each *prima facie* element of the defamation claim, notwithstanding the defendant's intent, so as to create a genuine issue of material fact *requiring* trial.[148] Of course, the "summary judgment" standard announced in *Cahill* is not the summary judgment standard as recognized by civil procedure. As the court explained:

> In deciding a motion for summary judgment, "a trial court shall examine the factual record and make reasonable inferences therefrom in the light most favorable to the nonmoving party to determine if there is any dispute of material fact." "[I]f from the evidence produced there is a reasonable indication that a material fact is in dispute or if it appears desirable to inquire more thoroughly into the facts in order to clarify application of the law, summary judgment is not appropriate." Thus, to obtain discovery of an anonymous defendant's identity under the summary judgment standard, a defamation plaintiff "must submit sufficient evidence to establish a *prima facie* case for each essential element of the claim in question." In other words, the defamation plaintiff, as the party bearing the burden of proof at trial, must introduce evidence creating a genuine issue of material fact for all elements of a defamation claim *within the plaintiff's control.*[149]

In short, under the *Cahill* summary judgment standard, a defamed plaintiff must present enough evidence supporting each prima facie element of his claim to justify proceeding to trial.

---

[147] *Id.*

[148] *Cahill*, 884 A.2d at 458 (emphasis added). The court noted that it did "not rely on the nature of the Internet as a basis to justify [its] application of the legal standard." *Id.* at 465. Therefore, the summary judgment standard is applied in Delaware whenever a defamation plaintiff seeks the identity of an anonymous defendant, regardless of the communicative medium. *Id.*

[149] *Id.* at 462-63 (citations omitted) (emphasis in original).

In adopting the summary judgment standard, the court reasoned that it had not "set the bar too high"[150] because the plaintiff is required only to address those elements of the defamation claim within his or her control.[151] Therefore, under the summary judgment standard, a public figure plaintiff is *not* required to produce evidence of actual malice, since "without discovery of the defendant's identity, satisfying this element may be difficult, if not impossible."[152]

Applying the summary judgment standard to the facts of the case, the court found that any reasonable person would have found that Doe's statements were merely opinion.[153] Because Cahill failed to establish the first element of his defamation claim, the court reversed the trial court's order compelling disclosure of Doe's identity.[154]

B. Beyond the Courts: Commentator Suggestions for Resolving the Section 230 Dilemma

While most courts to address the issue have cited *Dendrite*'s "sufficient evidence" standard[155] or *Cahill*'s "summary judgment" standard[156] approvingly, commentators have continued to suggest alternative remedies. For example, one commentator has analogized ISPs under section 230 to journalists who are subpoenaed for sources and assert their journalistic

---

[150] *Id.* at 462.

[151] *Cahill*, 884 A.2d at 463.

[152] *Id.* at 464.

[153] *Id.* at 467.

[154] *Id.* at 467-68.

[155] *See supra* note 130.

[156] *See* In re Does 1-10*,* 242 S.W.3d 805 (Tex. App. 2007); McMann v. Doe, 460 F.Supp.2d 259 (D. Mass. 2006); Best Western Inter'l v. Doe, No. CV-06-1537-PHX-DGC, 2006 WL 2091695 (D. Ariz. 2006); *see also* Vincent, *supra* note 105 at 1005 (advocating that litigants and courts adopt the *Cahill* summary judgment standard, which "provides for better judicial efficiency." *Id.* at 1003.); *but see* S. Elizabeth Malloy, *Anonymous Bloggers and Defamation: Balancing Interests on the Internet*, 84 Wash. U. L. Rev. 1187, 1191 (2006) (criticizing the *Cahill* standard for "fail[ing] to look at the repercussions for those who fall victim to these online anonymous bloggers." *Id.* at 1191.).

privilege.[157] She suggests using *Branzberg v. Hayes*[158] and its progeny to analyze, on a case-by-case basis, whether disclosure of an anonymous defendant's identity should be compelled.[159] In online defamation cases, this would require the plaintiff to prove "that the information sought is relevant, goes to the heart of the [plaintiff's] claim, and is unavailable from any other source."[160]

More recently, a commentator has turned to the DMCA, particularly section 512,[161] as a source of guidance. Olivera Medenica has proposed the Online Defamation Limited Liability Act ("ODEFLLA").[162] ODEFLLA is a suggested amendment to section 230 of the CDA that would include: "(1) a safe harbor provision . . . including a notice and takedown provision for allegedly infringing or defamatory material; (2) limited liability for Internet intermediaries by providing a statutory cap on damages; and (3) a public Internet intermediary defense fund as insurance against unwarranted liability."[163] Under ODEFLLA, upon receiving notice of an allegedly defamatory statement, ISPs would be required to remove the defamatory statement for a finite period, contact the content creator and explain why the material was taken down, and forward notice of removal to the complaining party.[164] Thereafter, the plaintiff would have a limited period of time in which to file a lawsuit for defamation.[165] If the plaintiff fails to file

---

[157] *See* Sunkel, *supra* note 96, at 1214.

[158] Branzberg v. Hayes, 408 U.S. 665 (1972).

[159] *See Sunkel*, *supra* note 96, at 1215-16.

[160] *Id.* at 1218.

[161] 17 U.S.C. § 512 (2006).

[162] *See* Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 263 (2007).

[163] *Id.*

.

[164] *Id.* at 265-66. This notice and takedown provision is based loosely on 17 U.S.C. § 512(c).

[165] *Id.* at 266.

during this window, the material could then be republished online.[166] Thus, an ISP would be required to show that it qualified under section 230 and that it had satisfied the notice and takedown provisions of ODEFLLA before a court would grant the ISP the immunity contemplated in section 230 as it currently exists.[167] The purpose of ODEFLLA then is to clarify what role ISPs must assume when notified of a defamatory statement on their service, and to protect injured plaintiffs by subjecting ISPs to liability if they fail to meet certain conditions in contacting the alleged John Doe defamer.[168]

Each of these proposals offers an interesting solution to a problem that has perplexed courts for more than a decade. A closer look at the journalist-privilege approach, however, reveals that it is too similar to the *America Online* "good faith" approach, which critics argue suppresses speech. Indeed, proving "that the information sought is relevant, goes to the heart of the [plaintiff's] claim, and is unavailable from any other source"[169] mirrors the *America Online* good faith standard which requires "that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and . . . the subpoenaed identity information is centrally needed to advance that claim."[170] Were courts to apply the journalistic-privilege or *America Online* standards, frivolous defamation suits could be filed simply to reveal the identity of an alleged defamer, and used to harass him or her. As the *Cahill* court noted, a defamation plaintiff could obtain the identity of

---

[166] *Id.*

[167] Medenica & Wahab, *supra* note 162, at,267.

[168] *Id.* at 265-66.

[169] Sunkel, *supra* note 96, at 1218.

[170] *In re Subpoena Duces Tecum to Am. Online*, 2000 WL 1210372, at *8.

the alleged defamer under the good faith standard even if his case were not very strong.[171] Then, "[a]fter obtaining the identity of an anonymous critic . . . a defamation plaintiff who either loses on the merits or fails to pursue a lawsuit is still free to engage in extra-judicial self-help remedies; more bluntly, the plaintiff can simply seek revenge or retribution."[172] These low standards could possibly have a chilling effect on anonymous speech, or even increase the amount of defamatory material posted to the Internet in retaliation. Similarly, by potentially opening up ISPs to even liability for their subscriber's defamatory statements, ODEFLLA usurps the primarily legislative intent of section 230. Moreover, responding to every request for takedown could potentially burden ISPs, and lead to a policing of the Internet that Congress was attempting to avoid through section 230's enactment.

IV. THE "GOOD SAMARITAN AMENDMENT"

In turn, I too purpose an amendment to section 230 of the CDA. *Cahill*'s summary judgment standard has been cited favorably by courts and commentators alike, primarily because it most effectively balances the competing interests of injured plaintiffs, anonymous speakers, and Congress' original intent in enacting section 230.[173] Therefore, to increase judicial efficiency, I suggest that the *Cahill* summary judgment standard be codified as an amendment to the CDA.

This would not be the first time that Congress has codified a subpoena standard for ISPs. In fact, section 512(h) of the DMCA – enacted two years after the CDA – sets forth a procedure for subpoenaing ISPs to disclose the identities of alleged copyright infringers.[174] Under section

[171] *Cahill*, 884 A.2d at 457.

[172] *Id.*

[173] *See supra* note 156 for cases and commentaries approving the *Cahill* standard.

[174] *See* 17 U.S.C. § 512(h) (2006).

512(h), a copyright owner must submit three items along with its request that the clerk issue a subpoena: (1) a notice identifying the copyrighted works alleged to have been infringed, including information reasonably sufficient for the ISP to locate the material, as required by section 512(c)(3)(A); (2) a proposed subpoena; and (3) a sworn declaration that the subpoena will be used "to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights" under federal copyright law.[175] If the copyright owner's request is properly prepared, and includes the above items, the clerk will sign the proposed subpoena and return it to the copyright owner for delivery to the ISP.[176] Upon receiving the subpoena, the ISP is required to disclose to the copyright owner the information required by the subpoena.[177] A caveat to section 512(h) subpoena – intended by Congress or not – is that a subpoena to identify alleged copyright infringers may only be issued to an ISP that stores infringing materials on its servers, not to an ISP that acts as a mere conduit for the data transferred between its users.[178]

The proposed "Good Samaritan Amendment" to section 230 of the CDA operates much like the subpoena provision in section 512(h) of the DMCA, except its language is crafted in light of the *RIAA v. Verizon* opinion to apply to all ISPs, regardless of whether they store or act as a mere conduit for the transfer of defamatory materials. In essence, the "Good Samaritan Amendment" seeks to combine the technical aspects of section 512(h) of the DMCA with the

---

[175] 17 U.S.C. § 512(h)(2).

[176] 17 U.S.C. § 512(h)(4).

[177] 17 U.S.C. § 512(h)(5).

[178] *See* Recording Indus. Ass'n of Am. v. Verizon, 351 F.3d 1229, 1236 (D.C. Cir. 2003) (holding that a subpoena to an ISP acting as a mere conduit cannot meet the notice requirement of section 512(c)(3)(A)(iii), and therefore cannot be the subject of a section 512(h) subpoena); *see also* In re Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945 (M.D.N.C. 2005).

Cahill summary judgment standard. While this note specifically focuses on online defamation, the "Good Samaritan Amendment" would apply to privacy torts generally, since those torts are often brought in conjunction with each other. The proposed language, including a necessary definition, follows:[179]

> **(f) Definitions.** –
>
> As used in this section:
>
> (5) Anonymous tortfeasor
>
> The term "anonymous tortfeasor" means any information content provider whose legal name is unascertained that, under any State law, allegedly commits any of the following torts: defamation, invasion of privacy, false light, appropriation, intrusion, or public disclosure of private facts.
>
> **(g) Subpoena to identify anonymous tortfeasor.** –
>
> (1) A plaintiff in a tort action or a person authorized to act on the plaintiff's behalf may request the clerk of any United States court to issue a subpoena to an interactive computer service for identification of an anonymous tortfeasor in accordance with this subsection.
>
> **(2) Contents of requests.** – The request may be made by filing with the clerk –
>
> (A) identification of the material alleged to be tortious, and information reasonably sufficient to permit the interactive computer service to locate the material;
>
> (B) a proposed subpoena;
>
> (C) evidence supporting each prima facie element of the claim for which the anonymous tortfeasor's identification is sought, sufficient to withstand a motion for summary judgment under Federal Rule of Civil Procedure rule 56 or compatible State law;
>
> (i) Notwithstanding the other requirements of subsection (B), where a prima facie claim includes an intent element, no evidence supporting the anonymous tortfeasor's intent is necessary.
>
> (D) a statement that the information in this subsection is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the plaintiff;

[179] Sequentially, the "Good Samaritan Amendment" proposed here follows the existing provisions of section 230, thus becoming section 230(g). I have also included a definitional amendment to section 230(f).

(E) a physical or electronic signature of a person authorized to act on behalf of the plaintiff; and

(F) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an anonymous tortfeasor and that such information will only be used for the purpose of properly serving that person as a defendant in any state tort action listed in subsection (f)(5).

(3) Basis for granting subpoena. – If each subsection of (g)(2) is satisfied, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the interactive computer service.

(4) Contents of subpoena. – The subpoena shall authorize and order the interactive computer service receiving the subpoena to expeditiously disclose to the plaintiff or person authorized by the plaintiff information sufficient to identify the anonymous tortfeasor to the extent that such information is available to the interactive computer service.

(5) Actions of interactive computer service receiving subpoena. – Upon receipt of the issued subpoena, the interactive computer service shall expeditiously disclose to the plaintiff or a person authorized by the plaintiff the information required by the subpoena, notwithstanding the requirements of section 551[180] of this title, or any other provision of law.

(6) Rules applicable to subpoena. – Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure, or compatible State law, governing the issuance, service and enforcement of subpoenas duces tecum.

Proposed section 230(g)(1) operates similarly to section 512(h)(1) of the DMCA,[181] and authorizes a plaintiff to seek the identity of their anonymous online defamer. Proposed section 230(g)(2), like section 512(h)(2) of the DMCA, sets out the items a plaintiff must file with the clerk when requesting a subpoena. Specifically, a plaintiff must provide: (1) identification of the material alleged to be tortious, to aid the ISP in identifying the anonymous tortfeasor, as required

[180] Referring to 47 U.S.C. § 551(c)(2)(B) (2006); *see supra* note 104.

[181] 17 U.S.C. § 512(h)(1).

by part one of the *Cahill* summary judgment standard;[182] (2) a proposed subpoena;[183] (3) evidence supporting each prima facie element of the tort claim for which the plaintiff is seeking the anonymous tortfeasor's identity – notwithstanding evidence of intent – as required by part two of the *Cahill* summary judgment standard;[184] (4) a statement that the information submitted is accurate;[185] (5) the signature of the plaintiff or her authorized agent;[186] and (6) a sworn declaration stating that the subpoena is sought to identify an anonymous tortfeasor, and that such information will only be used for the purpose of properly serving that person as a defendant in a privacy tort action.[187] Thereafter, subsections (g)(3) – (6) of the "Good Samaritan Amendment" largely mirror subsections (h)(3) – (6) of the DMCA subpoena provision.[188]

Codifying *Cahill*'s summary judgment standard will provide for greater judicial efficiency by eliminating most subpoena hearings, while still being protective of the First Amendment interest in free, anonymous speech. For example, if a plaintiff's defamation claim has merit, the clerk of the appropriate court will issue the subpoena, and the ISP will be required to release the identity of the John Doe defamer, without a costly and timely proceeding. Moreover, if the anonymous defamer wishes to challenge the subpoena, he will know up front what comments the plaintiff alleges are defamatory and the legal basis for the plaintiff's claim, including evidence supporting each prima facie element of the claim. If the anonymous defendant agrees to release his identity, he may do so, and thereafter challenge the evidence used

[182] *Compare with* 17 U.S.C. § 512(h)(2)(A); *see Cahill*, 884 A.2d at 461.

[183] *Compare with* 17 U.S.C. § 512(h)(2)(B).

[184] *See Cahill*, 884 A.2d at 461.

[185] *Compare with* 17 U.S.C. § 512(c)(3)(A)(vi).

[186] *Compare with* 17 U.S.C. § 512(c)(3)(A)(i).

[187] *Compare with* 17 U.S.C. § 512(h)(2)(C).

[188] *See* 17 U.S.C. § 512(h)(3)-(6).

to support the plaintiff's prima facie showing, or argue that the plaintiff cannot show that he acted with the requisite intent. In contrast, tort claims without merit will be dismissed early in litigation. For example, if the plaintiff fails to provide adequate evidence supporting that the allegedly defamatory statement is false, as required by proposed subsection (g)(2)(C), the clerk will simply refuse to issue the subpoena and the John Doe's identity will remain protected.

In addition to protecting defamed plaintiffs and the right to speak anonymously, codifying the *Cahill* summary judgment standard promotes the public policy Congress intended through the original "Good Samaritan" provision. In enacting the CDA as a whole, Congress intended to protect Internet users;[189] in enacting section 230(c), the "Good Samaritan" provision, Congress' purpose was to protect ISPs from liability. As currently enacted, the "Good Samaritan" provision fails to live up to its name. Indeed, ISPs are protected, but the defamed are not.

The proposed "Good Samaritan Amendment" keeps intact Congress' intent to limit ISP liability, while also making ISPs "Good Samaritans" by requiring them to release the identities of online defamers to those whose lives are shaken by truly defamatory statements on the Internet. As such, the proposed amendment corrects the misnomer of section 230, by protecting plaintiffs without expanding ISP liability and without infringing our most revered First Amendment rights.

CONCLUSION

Internet defamation, more than hyperbole or mere opinion, is a serious matter. As demonstrated by the pending *Ciolli* case, online defamation can ruin reputations, or worse, as demonstrated by the *Zeran* case, put lives at risk. As currently enacted, CDA section 230 fails to

[189] Albeit only minors from Internet pornography, but Congress could not have foreseen the boom in Internet defamation.

accommodate meritous defamation claims by failing to announce standards for when an ISP – insulated from liability under the section – must identify its subscribers who defame others anonymously. Codifying *Cahill*'s summary judgment standard will bring quick resolution to a problem that has plagued courts for more than ten years. As the Web continues to expand, so will the "Sleazy Z's" and "Ayatollah of Rock-n-Rollah's" who may defame online. The proposed "Good Samaritan Amendment" to section 230 of the CDA is a possible solution, one that keeps ISPs free from liability, protects the First Amendment right to speak anonymously online, and allows those who are truly defamed to seek the legal recourse to which they are entitled.