Florida Journal of International Law

Volume 27 | Issue 2 Article 4

January 2015

Realism About Remedies and the Need for a CDA Takedown: A Comparative Analysis of § 230 of the CDA and the U.K. Defamation Act 2013

Amanda Bennis

NOTE

REALISM ABOUT REMEDIES AND THE NEED FOR A CDA TAKEDOWN: A COMPARATIVE ANALYSIS OF § 230 OF THE CDA AND THE U.K. DEFAMATION ACT 2013

*Amanda Bennis**

* Amanda Bennis is an Associate in the Corporate and Securities Department at Stearns Weaver Miller Weissler Alhadeff & Sitterson, P.A. She graduated in 2015 with her J.D. from the University of Florida Levin College of Law. The author would like to thank Professors Lyrissa Barnett Lidsky and Elizabeth Lear at the University of Florida Levin College of Law for their assistance, comments, guidance, and encouragement throughout the Note writing process. The author would also like to thank her family for their love and support.

I. INTRODUCTION

Jane Doe logs onto ProfessionalNetworking.com, a website forum where professionals can network with other professionals around the world. She discovers a defamatory post saying, "Jane Doe is a cheating slut who cannot be trusted." Jane wants the defamatory statement taken down from the website. In the United States, Jane cannot get the statement taken down, yet had Jane lived in the United Kingdom, she would be able to get the statement taken down.

The problem encountered by the above victim of cyber defamation is the limited avenues for relief in the United States, specifically the lack of a takedown remedy. Cyber misconduct victims sometimes have the ability to pursue a civil remedy against the author of a defamatory statement provided the author's identity is ascertainable.[1] However, the Internet has presented a unique problem in that cyber victims face difficult statutory, judicial, and technological obstacles in seeking the takedown of the defamatory statement from the Internet. Notably, victims of cyber misconduct are generally precluded from bringing suit against the interactive computer service provider (ISP)[2] to seek the removal of

1. *See* Tara E. Lynch, *Good Samaritan or Defamation Defender? Amending the Communications Decency Act to Correct the Misnomer of § 230 . . . Without Expanding ISP Liability*, 19 SYRACUSE SCI. & TECH. L. REP. 1, 17 (2008) ("For plaintiffs who could identify their online defamer, the loss was simply monetary.").

2. 47 U.S.C. § 230(f)(2) ("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."). The courts have interpreted ISP "to include all intermediaries," especially website operators. Nancy S. Kim, *Website Design and Liability*, 52 JURIMETRICS J. 383, 393 (2012) (citing Fair Hous. Council of San Fernando Valley v. Roommates.com LLC, 521 F.3d 1157, 1161–63 (9th Cir. 2008) & Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065 (C.D. Cal. 2002)).

the defamatory statement.[3] As the number of Internet users steadily increases,[4] there has been a corresponding increase in the amount of online defamation.[5]

Section 230 of the Communications Decency Act (CDA), which regulates the Internet and ISP liability, serves as a statutory obstacle to the ultimate goal of a victim of cyber defamation of restoring his or her reputation.[6] Specifically, § 230 precludes cyber defamation victims, as well as all plaintiffs from bringing suit against the ISP, for either civil or equitable relief, as the publisher or distributor of the defamatory content.[7] Section 230 has enabled the Internet to become a forum where people, behind the safety of their computer screens or smart phones, have the ability to post defamatory content without any regard for the consequences of their conduct or the subsequent harm to the victim's reputation.[8] In fact, the "judiciary's inflated interpretation of § 230 has created a legal environment that is ideal for injury and difficult for redress."[9] Although there is general agreement among legal scholars that § 230 should be updated to address the unique aspects of the Internet and include a takedown remedy for cyber misconduct,[10] currently, no U.S.

---

3. *See* 47 U.S.C. § 230; David S. Ardia, *Freedom of Speech, Defamation, and Injunctions*, 55 WM. & MARY L. REV. 1, 16 (2013) ("§ 230 . . . grants . . . [ISPs] broad protection from defamation claims based on the speech of third parties, including protection from injunctive relief.").

4. A recent statistic has shown that global Internet use has increased 566.4% from 2000 to 2012. Internet World Stats: Usage and Population Statistics, Internet Usage Statistics: The Internet Big Picture, http://www.internetworldstats.com/stats.htm (last visited Feb. 23, 2014).

5. *See* Ardia, *supra* note 3, at 11 ("Today, bloggers, users of social media, and 'citizen journalists' are more often the targets of defamation claims.").

6. *See id.* at 15–16 ("A study conducted in the 1980s . . . found that only 20 percent of plaintiffs sued to obtain money as compensation for their reputational harms. Instead, . . . what libel plaintiffs desire most is a correction or retraction.").

7. *See* 47 U.S.C. § 230; David E. Hallett, *How to Destroy a Reputation and Get Away with it, the Communication Decency Act Examined: Do the Policies and Standards Set Out in the Digital Millennium Copyright Act Provide a Solution for a Person Defamed Online*, 41 IDEA 259, 274 (2001) ("The CDA statutorily limits ISP liability by making it impossible to find an essential element of the claim, publication.").

8. "The CDA does not adequately protect society from would be online defamers." Hallett, *supra* note 7, at 277. Sarah H. Ludington, *Aiming at the Wrong Target: The "Audience Targeting" Test for Personal Jurisdiction in Internet Defamation Cases*, 73 OHIO ST. L.J. 541, 542 (2012) ("With a few keystrokes, I can publish an injurious falsehood accessible to anyone in the world with an Internet connection and the desire to read it.").

9. Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 341 (2005). "ISPs have no obligation to remove tortious materials, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers." *Id.*

10. *See* Allison E. Horton, *Beyond Control?: The Rise and Fall of Defamation Regulation on the Internet*, 43 VAL. U. L. REV. 1265, 1314 (2009) (discussing how the Internet's development

scholar fully analyzes the practical aspects of implementing and enforcing a takedown decree for post-publication defamatory speech.[11]

Conversely, other countries[12] have enacted takedown provisions to provide remedies for cyber defamation. Notably, the United Kingdom recently passed the U.K. Defamation Act 2013[13] which reformed U.K. defamation law to account for the uniqueness of the Internet and its pervasive use throughout society. The U.K. Defamation Act 2013 provides website operators a defense from liability[14] while also providing U.K. courts with the power to require a website operator to take down defamatory content.[15]

This Article provides a proposed method for instituting a federal takedown remedy for a state tort without subjecting ISPs to liability. This proposed solution effectively balances a successful mechanism for remedying harm caused by cyber misconduct with allowing free speech and the continuing growth of the Internet as a popular medium for communication.

Part II examines the unique aspects of the Internet, provides a brief background of traditional defamation law, and discusses the current obstacles to recovery victims of cyber defamation encounter under § 230. Part III reviews the background of the CDA, judicial interpretation of § 230, and the growing dissatisfaction with the broad interpretation of § 230. Part IV studies the background of U.K. defamation law, the influence of the E.U. Electronic Commerce Directive on the creation of the U.K. Defamation Act 2013, and analyzes the pertinent sections of the U.K. Defamation Act 2013. Part V presents a proposed solution and framework for amending § 230 to include a federal takedown remedy. Part V also addresses jurisdictional or other potential concerns that could arise in response to the proposed solution.

---

and interplay with the CDA has "produced cries for reformation.").

11. One such problem with implementing a takedown decree is that defamation law is a state tort remedy and therefore creating a federal remedy creates a host of enforcement problems.

12. *See, e.g.*, Defamation Act 2013, c. 26 (U.K.); Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce') [hereinafter E.U. Electronic Commerce Directive] (directing E.U. Member States to create a notice and takedown requirement for Internet defamation).

13. Defamation Act 2013, c. 26 (U.K.); David Hooper et al., *Defamation Act 2013 – What Difference Will It Really Make?*, 24 ENT. L.R. 2013, 199, 205 (2013) ("The Act is a welcome and long overdue reform of the law of defamation.").

14. Defamation Act 2013, c. 26 § 5 (U.K.).

15. Defamation Act 2013, c. 25 § 13 (U.K.).

II. SECTION 230 OF THE CDA NEEDS TO BE AMENDED TO ADDRESS THE INTERNET'S IMPACT ON U.S. DEFAMATION LAW

The Internet is a medium of communication that presents unique legal concerns. The Internet is omnipresent throughout all facets of life in modern society.[16] It is concerning that the CDA, which regulates the Internet's use, has not been updated, since its passage eighteen years ago, to address the Internet's pervasive presence.[17] Accordingly, the expansive judicial interpretation of § 230 and the scope of § 230 immunity is now too broad in light of the unique aspects of the Internet and the growing inequities facing modern cyber defamation victims.

A. *Unique Aspects of the Internet*

The Internet's global presence enables easy accessibility of information to a mass audience.[18] This exponential spread of information[19] helped create a global culture that encourages people to impulsively share their every thought with the click of a button.[20] The Internet's function as a faceless medium creates a lack of accountability for online communications, for which editorial control and legal

16. *See* Phillip Adam Davis, *The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflicts of Law is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier*, 54 FED. COMM. L.J. 339, 348 (2002) ("Cyberspace is no longer a 'new frontier,' but a fixed communication device that is commonplace and woven into the fabric of American society.").

17. 47 U.S.C. § 230 (2006).

18. Scott Sterling, *International Law of Mystery: Holding Internet Service Providers Liable for Defamation and the Need for a Comprehensive International Solution*, 21 LOY. L.A. ENT. L. REV. 327, 347 (2001) ("[A]nything published on the Internet has the ability to reach a worldwide audience."). Further, the rapid growth of Internet users has increased the sheer volume of "mass" communications. MATTHEW COLLINS, THE LAW OF DEFAMATION AND THE INTERNET 3 (3d ed. 2010) (The Internet "brings mass communication to the mass: anyone with a computer and an Internet connection or, increasingly, an Internet-enabled device, can utilize its potential.").

19. "[T]he presently existing Internet within cyberspace functions to '[enable] people to communicate with one another with unprecedented speed and efficiency and is rapidly revolutionizing how people receive and share information.'" Kimberly Quon, *Implementing a Standard of Care to Provide Protection from a Lawless Internet*, 31 WHITTIER L. REV. 589, 606 (2010) (quoting Blumenthal v. Drudge, 992 F. Supp. 44, 48 (D.D.C. 1998)).

20. *See* Kim, *supra* note 2, at 400–01 (commenting that impulsive posting of content is one "regrettable online behavior" associated with modern online culture). The computer, smart phone, or other method of Internet access serves as a shield, to embolden people to say more, than they would in face-to-face interactions. *See* Jennifer Benedict, *Deafening Silence: The Quest for a Remedy in Internet Defamation*, 39 CUMB. L. REV. 475, 479 (2009) ("There are no gatekeepers in cyberspace and anyone with a computer is capable of targeting anyone else."); Doug Rendleman, *The Defamation Injunction Meets the Prior Restraint Doctrine* 19 (Wash. & Lee Pub. Legal Studies Research Paper Series, Working Paper No. 2014-8, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2404560 ("People who previously lacked access to widespread communication can now scream vitriol from their virtual rooftops.").

regulation is difficult.[21] Further, once defamatory content appears on the Internet, it is difficult to remove[22] due to the advent of mirror websites[23] and the growing trend of ISPs to refuse to allow posters to remove content.[24]

Finally, the Internet stretches jurisdictional boundaries,[25] creating additional obstacles for cyber victims. Obtaining jurisdiction over the author of the defamatory content or the ISP becomes almost impossible, if neither the author nor the ISP is subject to the forum court's jurisdiction.[26] Defamation law is a state tort action, but the problem of cyber defamation is global in scope. Consequently, recognition and enforcement of a state tort defamation action both in the United States and in foreign countries is problematic.[27] All the characteristics that make the Internet an appealing medium of communication, "also make [the Internet] a devastatingly effective tool to ruin the lives of innocent citizens."[28] Thus, in light of the Internet's pervasiveness and the expansive immunity provided to ISPs under § 230, the quantum of harm suffered by cyber defamation victims is greater than the quantum of harm suffered by defamation victims in other mediums of communication.[29]

---

21. *See* Rendleman, *supra* note 20, at 19 ("Observers think that social media, like alcohol, is disinhibiting because it undermines judgment and exacerbates impulsive and emotional responses."); *see* Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn From John Doe?*, 50 B.C. L. REV. 1373, 1375 (2009) [hereinafter Lidsky, *John Doe*].

22. Terence J. Lau, *Towards Zero Net Presence*, 25 NOTRE DAME J.L. ETHICS & PUB. POL'Y 237, 242 (2011) ("scrubbing content becomes more and more difficult as time progresses and the content replicates."); *see* Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1112 (2011) [hereinafter Lipton, *Victimization*] ("Even where information about a victim is removed from one website, it may be cached and copied on other websites.").

23. Mirror websites publish "the same files, format, and HTML as the original website." Phil Cameron, *Internet Travel Purchases*, 30 NO.3 GPSOLO 48, 53 (2013). The purpose of a mirror website is to ensure "the site is available from more than one location—[for] sites at risk of being hacked or banned." John Alan Farmer, *The Spector of Crypto-Anarchy: Regulating Anonymity-Protecting-Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 740–41 (2003).

24. *See* Kim, *supra* note 2, at 415–16; Lidsky, *John Doe*, *supra* note 21, at 1390.

25. *See* Yuval Karniel, *Defamation on the Internet – A New Approach to Libel in Cyberspace*, 2 J. INT'L MEDIA & ENT. L. 215, 220 (2009) (noting the Internet is "[w]ithout geographical borders.").

26. *See* Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, A Suggested Approach*, 6 RICH. J.L. & TECH. 9, *8 (1999) (noting that determining jurisdiction for cyber-libel cases can present several difficulties for plaintiffs); Amanda Groover Hyland, *The Taming of the Internet: A New Approach to Third-Party Internet Defamation*, 31 HASTINGS COMM. & ENT. L.J. 79, 109 (2008) ("These problems are compounded by the wide range of possible jurisdictions where a web operator may be called into court[.]").

27. *See* 28 U.S.C. §§ 4101–05; *see generally* Bruce D. Brown & Clarissa Pintado, *The Small Steps of the Speech Act*, 54 VA. J. INT'L L. DIG. 1 (2014).

28. Lau, *supra* note 22, at 253.

29. *See* Robert D. Richards, *Sex, Lies, and the Internet: Balancing First Amendment Interests, Reputational Harm, and Privacy in the Age of Blogs and Social Networking Sites*, 8 FIRST AMEND. L. REV. 176, 212 (2009) ("[the] ability to disseminate potentially damaging and

B. *Defamation and the Internet*

As the Internet's popularity grows, there is an increasing amount of online defamation.[30] The tort of defamation is designed to provide remedies to defamation victims, however the application of the tort to the Internet is inadequate because it fails to provide sufficient remedies for cyber defamation victims.[31] In order to fully understand why § 230 needs to be amended to include a takedown remedy for cyber defamation, it is essential to understand the tenets of defamation law, both common law foundations and constitutional limitations, as well as current obstacles to recovery.

1. Traditional Elements of Defamation

The defamation[32] tort provides a mechanism for individuals to recover for harm to their reputation.[33] The tort reconciles "the competing interests of freedom of expression and the protection of individual reputation."[34] In order for a plaintiff to prevail under the common law, the plaintiff had to prove: (1) the existence of a defamatory communication;[35] (2) identification of the plaintiff to a third party;[36] and (3) publication of the communication to at least one third party.[37] The United States Supreme Court in *New York Times Co. v. Sullivan* constitutionalized the tort of

---

false information about another to a mass audience with little more than a keystroke's worth of effort threatens to devalue reputation to a point never before experienced in American culture."). *See also* Lipton, *Victimization*, *supra* note 22, at 1116 ("Much online conduct will damage a victim's reputation permanently with little recourse because many laws are focused on physical world conduct rather than online communications.").

30. *See* Ardia, *supra* note 3, at 12 ("[A]necdotal evidence indicates that defamation claims are actually increasing.").

31. *See id.* at 18 ("Not surprisingly, defamation plaintiffs are frustrated with the remedies available to them.").

32. "The term 'defamation' encompasses the twin torts of libel and slander." LYRISSA BARNETT LIDSKY & R. GEORGE WRIGHT, FREEDOM OF THE PRESS: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION 63 (Jack Stark ed. 2004) [hereinafter LIDSKY, FREEDOM OF THE PRESS].

33. *See id.* Moreover, "[p]ublic 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." Lynch, *supra* note 1, at 6.

34. COLLINS, *supra* note 18, at 4.

35. A defamatory statement is "a statement that tends to harm an individual's reputation in the eyes of his or her community. LIDSKY, FREEDOM OF THE PRESS, *supra* note 32, at 66. The court will "'presume[] damages' based solely on the nature of the defamatory statements." *Id.*

36. *Id.*

37. ROBERT D. SACK, SACK ON DEFAMATION: LIBEL, SLANDER, AND RELATED PROBLEMS 2-70 (PLI, 3d ed. 1999). Publication occurs when defamatory words are "expressed purposely or negligently to a third party." *Id.* (citing Lyons v. Nat'l Car Rental Sys., 30 F.3d 240, 244 (1st Cir. 1994)).

defamation[38] and added two additional elements for the plaintiff to prove: (4) falsity of the communication;[39] and (5) some type of fault of the defendant, such as actual malice or negligence.[40]

Additionally, there are three types of secondary liability in a defamation action: publisher (re-publisher) liability, distributor liability, and common carrier (or conduit) liability.[41] Both re-publisher liability[42] and distributor liability[43] are relevant to the problem of cyber defamation. The key distinction between re-publisher and distributor liability is that a critical element for the imposition of distributor liability is a finding by the court that the party (distributor) had notice that the statement was defamatory.[44] Yet the question when addressing cyber defamation and ISP liability is "whether the traditional law of defamation 'fits' the Internet."[45]

2. Obstacles to Recovery in Internet Defamation Cases

Prior to the passage of § 230 of the CDA, many legal scholars initially believed courts would apply defamation law to the Internet in the same manner courts applied it to all other print medium.[46] This belief included

38. N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

39. *Id.* Proving the truth of the statement used to be a defense to defamation; now proving the statement's falsity is incorporated into the elements a plaintiff must prove. LIDSKY, FREEDOM OF THE PRESS, *supra* note 32, at 74; Phila. Newspapers, Inc. v. Hepps, 475 U.S. 767 (1986).

40. *See N.Y. Times*, 376 U.S. 254. The fault of the defendant varies based on whether the plaintiff is a public official or public figure versus a private figure. *See* LIDSKY, FREEDOM OF THE PRESS, *supra* note 32, at 66–74.

41. Amanda Groover Hyland, *The Taming of the Internet: A New Approach to Third-Party Internet Defamation*, 31 HASTINGS COMM. & ENT L.J. 79, 81 (2008) ("Those who republish a libelous statement do not escape liability simply because they did not originally create the content.").

42. Liberty Lobby, Inc. v. Dow Jones & Co., 838 F.2d 1287, 1298 (D.C. Cir. 1988); RESTATEMENT (SECOND) OF TORTS § 578.

43. RESTATEMENT (SECOND) OF TORTS § 581 (Distributor liability occurs when a person "only delivers or transmits defamatory matter published by a third person.").

44. *Id.*

45. Bryan P. Werley, *Aussie Rules: Universal Jurisdiction Over Internet Defamation*, 18 TEMP. INT'L & COMP. L.J. 199, 220–21 (2004) ("Whether the technical definition of publication with regards to defamation can really be applied to the Internet, which is unlike anything else the common law definition has been applied to, both in terms of its reach and the way in which it is accessed.").

46. *See* Sean P. Trende, *Defamation, Anti-SLAPP Legislation, & the Blogosphere: New Solutions for an Old Problem*, 44 DUQ. L. REV. 607, 619 (2006); *see also* Jeffrey M. Tayler, *Liability of Usenet Moderators for Defamation Published by Others: Flinging the Law of Defamation into Cyberspace*, 47 FLA. L. REV. 247, 267 (1995) (acknowledging that many legal commentators asserted that traditional standards of defamation law would still apply to the Internet).

the availability of traditional defamation remedies such as damages[47] and equitable relief such as an apology, a retraction of the statement,[48] or in limited cases an injunction.[49] However, the Internet's global scope and § 230 immunity provide obstacles to the availability of remedies in cyber defamation cases.

First, the Internet's global structure creates an obstacle to the ability of a victim of cyber defamation to ensure the court has jurisdiction over the claim and the parties.[50] In many situations, the case begins and ends with a determination as to whether the court has jurisdiction to adjudicate the matter.[51] Moreover, determining personal jurisdiction has proven to be a "difficult proposition" for victims of cyber defamation[52] as the test courts use for evaluating jurisdiction differs based upon each state or federal court.[53] Thus, the ability of a court to exercise jurisdiction over a local or foreign ISP for a state tort claim presents an obstacle to the institution of recovery proceedings, as the Internet's reach has no set boundaries.

Even if a court were able to assert jurisdiction over an ISP, the remedies available for prevailing cyber defamation plaintiffs are inadequate.[54] Specifically, § 230 ISP immunity prevents plaintiffs from joining the ISP as a party to the lawsuit.[55] At best, provided the plaintiff

---

47. *See generally* RESTATEMENT (SECOND) OF TORTS §§ 620–23 for a discussion of the types of damages a defamation plaintiff could seek.

48. *Id.* at 11–13 ("Legislatures of thirty-three states have enacted statutes that govern the procedure to be followed in demanding and publishing revocation."). However, there is "no judicial authority for right of retraction absent the existence of an applicable statute." *Id.* at 10–56.

49. *See* Ardia, *supra* note 3, at 48–51; *See generally* Tory v. Cochran, 544 U.S. 734, 738 (2005).

50. *See* Ludington, *supra* note 8, at 543 (there is a "jurisdictional safe harbor (ironically) provided by the very ubiquity of the Internet.").

51. Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337, 1365 (2012) [hereinafter Lipton, *Intermediated Information Exchange*].

52. Waldman, *supra* note 26, at *8.

53. *Id.* at *9–15 (the tests range from totality of the contacts, effects test approach, and the Keeton test); *Id.* ("courts usually decline to exercise jurisdiction over interstate or foreign defendants where the principal or only connection with the forum state is that it is the place of residence of the plaintiff."); COLLINS, *supra* note 18, at 593–95 (However, courts will exercise jurisdiction in situations where there is a manifest intent by the defendant to "target and focus on the forum," and when "commercial and other contacts [exist] between the defendant and the forum state.").

54. *See* Lidsky, *John Doe*, *supra* note 21, at 1389–90.

55. *See* Ardia, *supra* note 3, at 17 ("Unless these online intermediaries voluntarily remove the defamatory speech, a court cannot force them to do so."); Kraig J. Marton et al., *Protecting One's Reputation – How to Clear a Name in a World Where Name Calling is so Easy*, 4 PHX. L. REV. 53, 60 (2010) ("the Communications Decency Act insulates the owners of websites from liability for defamation, sometimes presenting unique challenges for the defamed party to get the remedy they are seeking.").

knows the identity of the poster of the defamatory statement,[56] a successful plaintiff will recover damages[57] and possibly a takedown decree against the poster. However, this decree does not guarantee that the defamatory content will be removed from the Internet, and damages fail to adequately compensate cyber defamation victims because damages do not restore a victim's online reputation or remove the defamatory statement from the Internet.[58]

III. THE CDA

The Internet has changed dramatically since Congress enacted the CDA. In order to fully understand why § 230 is outdated, it is important to understand the impact it had in changing the application of defamation law to the Internet, specifically the immunity § 230(c) provided ISPs.

A. *Intent Behind the Creation of the CDA*

Prior to 1996, the common law determined Internet defamation actions, and held ISPs responsible for moderating defamatory content posted on the website by a third party.[59] As a result of the perverse incentives created by two decisions, *Cubby, Inc. v. CompuServe, Inc.*[60] and *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, Congress felt compelled to intervene and pass the CDA.[61] Both cases had similar facts and were adjudicated within the state of New York, yet arrived at two completely different conclusions. In the first case, *Cubby*, the court held that the defendant was a distributor and therefore not liable for defamatory remarks posted on its forum boards.[62] In the second case,

56. *See* Lidsky, *John Doe*, *supra* note 21, at 1374.

57. *Id.* at 1389–90.

58. *See id.* ("Libel law gives successful plaintiffs compensatory and occasionally punitive damages, remedies that are virtually meaningless when the defendant has no money to satisfy a judgment.").

59. *See* Molly Sachson, *The Big Bad Internet: Reassessing Service Provider Immunity Under § 230 to Protect the Private Individual from Unrestrained Internet Communication*, 25 J. CIV. RTS. & ECON. DEV. 353, 357–58 (2011).

60. Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

61. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995), superseded by statute, Communications Decency Act of 1996, 47 U.S.C. § 230 (2006).

62. *See Cubby*, 776 F. Supp. at 141. In *Cubby*, defendant ISP CompuServe, provided its subscribers access to over thousands of information services and forums. *Id.* at 137. One such forum contained the publication "Rumorville USA" which plaintiffs claimed published "false and defamatory statements" about their competing business and the individual plaintiffs. *Id.* at 138. The Southern District of New York treated CompuServe as a distributor, finding that CompuServe did not moderate or filter the content that was posted. *Id.* at 141. Therefore, as CompuServe did not know or have reason to know of the defamatory content, CompuServe was not liable. *Id.*

Stratton, the court held that a similarly situated defendant was a publisher and liable for the defamatory content on its forum boards.[63]

Congress was concerned with the divergent results of the above two cases because Congress wanted to encourage ISPs to self-regulate the dissemination of material on their websites without fear of liability.[64] To address its concerns with the diverse incentives created by *Cubby* and *Stratton*,[65] Congress passed the Cox-Wyden Amendment to the Telecommunications Act of 1996.[66] The intent of the Cox-Wyden Amendment was to reverse the *Stratton* decision and to eliminate corresponding disincentives for intermediaries to screen content.[67] On February 8, 1996, the Communication Decency Act became effective as Title V of the Telecommunications Act of 1996.[68] The Cox-Wyden amendment was codified as § 230—Protection for private blocking and screening of offensive material—of the CDA.[69] The advent of § 230 was viewed as a successful merger of Congress's goals and of ensuring the continued growth of the Internet by providing protection for ISPs from liability for third-party comments.[70]

B. *The Ambiguity Created by § 230*

In retrospect, § 230's language was ambiguous and failed to provide

63. *See Stratton*, 1995 WL 323710 at *1-*2. *Stratton* was decided four years after *Cubby*. *Id.* In *Stratton*, the Supreme Court of New York, in a state court trial on facts similar to *Cubby*, held defendant Prodigy liable as a publisher of the defamatory statements the plaintiff complained were posted on one of Prodigy's bulletin boards. *Id.* at *1, *3, *6. The court granted the plaintiff's motion for partial summary judgment finding Prodigy was a publisher because Prodigy and its agents moderated the content on the bulletin boards. *Id.* Therefore, Prodigy was liable for any defamatory content posted on its websites by third parties. *Id.* at *1.

64. *See* 47 U.S.C. § 230(b)(4).

65. The Cox-Wyden Amendment was also designed to address Congress's concern with the ease of accessibility of the Internet to children, especially to pornography on the Internet. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 52–59 (1996).

66. *See* Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 315–16 (2011); Cannon, *supra* note 65, at 67.

67. *See* Wu, *supra* note 66, at 316; 47 U.S.C. § 230.

68. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as 47 U.S.C. §§ 230, 560, 561).

69. *Id.*; *see also* Wu, *supra* note 66, at 315–17. Congress's goals for passing § 230 include objectives designed "to promote the continued development of the Internet," to encourage the development of technology, and "to remove disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b). "Congress sought to encourage providers and users of Internet services to practice self-regulation with respect to offensive material." Jae Hong Lee, *Batzel v. Smith & Barrett v. Rosenthal: Defamation Liability for Third-Party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 470 (2004).

70. *See* Wu, *supra* note 66, at 316.

guidance as to the scope of intermediary (ISP) liability.[71] The main source of ambiguity originates in § 230(c), where Congress attempted to structure the provision in a manner that would effectively promote self-regulation of ISPs.[72] Section 230(c), also known as the "Good Samaritan" provision,[73] was designed to give ISPs special protections from liability for publishing third-party content.[74]

This additional protection for ISPs from re-publisher liability is a protection not provided to the print or broadcast mediums.[75] Section 230(c) provides a medium-specific protection and holds ISPs liable for content that may be properly attributed to it.[76] Thus, for an ISP to be liable, the ISP must be deemed an "information content provider" meaning "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[77]

The ambiguity in § 230(c) arises in determining whether the ISP qualifies for protection from liability, essentially whether the ISP is a

---

71. *Id.* at 317; 47 U.S.C. § 230.

72. 47 U.S.C. § 230(c). § 230(c) provides:

> (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).

Id.

73. In fact, § 230(c) is titled "[P]rotection for 'good samaritan' blocking and screening of offensive material." 47 U.S.C. § 230(c).

74. *Id.* Hong Lee, *supra* note 69, at 470 ("The CDA was designed to encourage self-regulation by permitting Internet service providers (ISPs) to exercise their editorial powers in regulating offensive material without incurring strict liability for defamation as publishers of third-party content.").

75. *See* Ardia, *supra* note 3, at 10–11 ("More recently, defamation law took on a decidedly medium-specific aspect when Congress passed § 230 of the Communications Decency Act, which granted operators and users of websites and other interactive computer services broad protection from defamation claims based on the speech of third parties.").

76. 47 U.S.C. § 230(c)(1).

77. 47 U.S.C. § 230(f)(3).

publisher[78] or "responsible" for the "creation or development" of the disputed defamatory content.[79] This determination is relevant because the language of § 230 only addresses publishers, and makes no reference whatsoever to "distributors."[80] Despite the confusion surrounding whether § 230(c) also included distributors, Congress neither amended § 230(c) nor provided guidance as to what the definition of "publisher" encompassed.

C. *Judicial Interpretation of § 230(c)—A Divergence from Congress's Underlying Objective and the Creation of Immunity for Both Publishers and Distributors*

The burden fell to the courts to interpret § 230(c) and the courts have broadly interpreted the scope of § 230(c) immunity.[81]

1. *Zeran v. America Online, Inc.*

A court first addressed the ambiguity of § 230(c)(1) in the seminal case of *Zeran v. America Online, Inc.*[82] In *Zeran*, the plaintiff Ken Zeran was the victim of an "unidentified third party's hoax" posting on an AOL bulletin board advertising the sale of "Naughty Oklahoma T-Shirts," six days after the April 1995 Oklahoma City bombing.[83] Following this "anonymously perpetrated prank," Zeran received a "high volume" of angry phone calls.[84] Zeran notified an AOL representative of the hoax and was assured the post would be removed, however additional messages continued to be posted on AOL boards and the harassment continued.[85] Zeran ultimately filed suit against AOL seeking to hold AOL liable as a distributor for the defamatory content posted by a third party.[86]

---

78. *See* Quon, *supra* note 19, at 597.

79. *See* 47 U.S.C. § 230(c).

80. *Id.*

81. *See* Sachson, *supra* note 60, at 359. In fact, "courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'" *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003); *see also* Sachson, *supra* note 59, at 360.

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

83. *Id.* at 329. The shirts featured "offensive and tasteless slogans" about the Oklahoma City bombing. *Id.* The hoax message instructed "those interested in purchasing a shirt to call" Ken and provided Zeran's phone number. *Id.*

84. *Id.* Zeran could not change his phone number to avoid the harassing phone calls because his phone number's availability was critical to "running his business out of his home." *Id.*

85. *Id.*

86. Zeran was unable to bring any "action against the party who posted the offensive messages," because the party's identity was unknown. *Id.* Zeran alleged that once "he notified

AOL asserted § 230 as an affirmative defense, and the district court granted AOL's motion for judgment on the pleadings, which Zeran appealed.[87]

The Fourth Circuit examined § 230 and held that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make [ISPs] liable for information originating with a third-party user of the service."[88] Accordingly, the court concluded that § 230(c)(1) "forbids the imposition of publisher liability on a[n] [ISP] for the exercise of its editorial and self-regulatory functions."[89] The court also rejected Zeran's argument that § 230 left "distributor liability intact."[90] The Fourth Circuit held that distributor liability is "merely a subset, or a species, of publisher liability, and is therefore also precluded by § 230."[91] Consequently, the court affirmed AOL's motion for judgment on the pleadings as it found that AOL fell "squarely" within the definition of publisher and was protected by § 230 from suit.[92]

The Fourth Circuit's analysis and interpretation of § 230 in *Zeran* has been extoled as *clarifying* the ambiguity surrounding the meaning of § 230(c), specifically the meaning of "publisher" for purposes of § 230(c)(1).[93] *Zeran* established a broad immunity for ISPs under § 230(c)(1), protecting service providers from virtually all liability for content "originating with third parties."[94] Moreover, the *Zeran* opinion set the basic foundation for distributor immunity by holding that the term "publisher" in § 230(c)(1) encompassed liability protection for both publishers and distributors.[95] *Zeran* remains the leading case on intermediary immunity.[96]

AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material." *Id.* at 330.

87. *Id.* at 329–30.

88. *Id.* at 330. The Fourth Circuit also recognized that Congress's purpose in enacting § 230 was to reverse the *Stratton* decision. *Id.*

89. *Id.* at 331.

90. *Id.* at 332.

91. *Id.* In rejecting Zeran's notice liability argument, the court found that "liability upon notice would defeat the dual purposes advanced by § 230 of the CDA" because such notice liability would deter service providers from self-regulating and increase incentives to restrict speech. *Id.* at 333.

92. *Id.* at 332.

93. *Id.*

94. *See Zeran*, 129 F.3d at 332–33; Mark D. Quist, *"Plumbing the Depths" of the CDA: Weighing the Competing Fourth and Seventh Circuit Standards of ISP Immunity Under Section 230 of the Communications Decency Act*, 20 GEO MASON L. REV. 275, 288 (2012).

95. *Zeran*, 129 F.3d at 332–33.

96. *See* David Lukmire, *Can the Courts Tame the Communications Decency Act? The Reverberations of* Zeran v. American Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 385 (2010) ("*Zeran* laid the groundwork for future expansive readings of section 230."); Varty Defterderian,

2. Post-*Zeran* and § 230 Immunity

Zeran created a national standard for the interpretation of § 230(c). Since *Zeran*, a majority of courts have followed its analysis.[97] Courts in the First,[98] Second,[99] Third,[100] Fourth,[101] Fifth,[102] Seventh,[103] Eighth,[104] Ninth,[105] Tenth,[106] and Eleventh[107] Circuits have followed *Zeran*'s holding and provided broad immunity to ISPs protecting them from both publisher and distributor liability.[108]

The courts developed a three-prong test to determine ISP immunity from liability pursuant to § 230(c)(1).[109] To be afforded § 230(c)(1) protection, the ISP must prove that: (1) the defendant website provider is an "interactive computer service" within the meaning of § 230(f)(2)[110]; (2) the plaintiff is seeking to hold the defendant website provider liable as the publisher;[111] and (3) the information was "provided by another

---

Fair Housing Council v. Roommates.com: A New Path for Section 230 Immunity, 24 BERKELEY TECH. L.J. 563, 570 (2009) ("*Zeran* remains the preeminent case on section 230 immunity.").

97. Notably, due to § 230 immunity protecting ISPs, there has been limited cyber defamation litigation reaching the federal circuit court level. Of the seventy federal circuit court cases that quote some portion of § 230, forty-five of the cases reference § 230(c)(1). Search of Westlaw database, March 24, 2015. Twenty-seven federal circuit court cases quote *Zeran*. Search of Westlaw database, March 24, 2015.

98. Universal Comm. Sys., Inc. v. Lycos, 478 F.3d 413, 417, 422 (1st Cir. 2007).

99. Ricci v. Teamsters Union Local 456, No. 14-1732, 2015 WL 1214476 (2d Cir. Mar. 11, 2015) (noting that the court was going to join the consensus of other courts that have applied to immunity provisions of the Communications Decency Act to a growing list of Internet-based service providers).

100. DiMeo v. Max, 248 Fed. Appx. 280, 282 (3d Cir. 2007); Green v. Am. Online, 318 F.3d 465, 471 (3d Cir. 2003).

101. Nemet Chevrolet v. Consumeraffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009).

102. Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008).

103. Chicago Lawyers Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

104. *See* Johnson v. Arden, 614 F.3d 785, 792 (8th Cir. 2010).

105. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1105–06 (9th Cir. 2009); *see* Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003).

106. *See* F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1195 (10th Cir. 2009); Ben Ezra, Weinstein & Co., Inc. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).

107. Whitney Info. Network, Inc. v. Xcentric Venture, LLC, 199 F. App'x 738, 739–40 (11th Cir. 2006); *see* Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321–22 (11th Cir. 2006).

108. "Circuit courts have interpreted the CDA to broadly immunize almost all interactive website operators from defamation actions stemming from third-party content." Andrew Bluebond, *When the Customer is Wrong: Defamation, Interactive Websites, and Immunity*, 33 REV. LITIG. 679, 684 (2014).

109. *See* Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers*, 8 U. PITT. J. TECH. L. & POL'Y 3 (2007).

110. *See* 47 U.S.C. § 230(c)(1), (f)(2).

111. *See* 47 U.S.C. § 230(c)(1).

information content provider" within the meaning of § 230(f)(3).[112] The *Zeran* opinion has become firmly entrenched with the analysis of § 230. Not only has *Zeran* influenced and shaped CDA case law, it has turned § 230(c)(1) into a formidable obstacle for cyber defamation plaintiffs to overcome.[113]

D. *Growing Dissatisfaction with the Broad Interpretation of § 230*

Section 230 falls short of accomplishing Congress's goal of encouraging ISPs to self-regulate. Although Congress assumed ISPs would engage in self-regulation, as § 230 does not require ISPs to self-regulate and protects ISPs from liability if they do not, Congress's goal of ISP self-regulation has not been achieved.[114] As one commentator noted, "[t]he conferral of section 230 immunity has led to egregious results, which make a mockery of the term *good Samaritan* when applied to certain websites."[115]

First, there is disagreement over the language of § 230 and whether the term "publisher" in § 230(c)(1) actually includes distributor liability.[116] On one side, judicial interpretation, starting with the Fourth Circuit's holding in *Zeran*, ignores the fact that the text of § 230 makes "no separate reference to distributors."[117] By disregarding Congress's decision to exclude "distributors" from the language of § 230, the courts have created a broad general immunity for ISPs that was not explicitly mentioned in § 230's text.[118] Critics of the *Zeran* interpretation note that one of Congress's express reasons for passing § 230 was to reverse the

---

112. *See* 47 U.S.C. § 230(c)(1), (f)(3).

113. *See* Ken S. Myers, *Wikkimunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 174 (2006) (noting the "expanding scope of § 230(c)(1)'s application to various potential 'gatekeepers' of Internet content . . . .").

114. *See* Sewali K. Patel, *Immunizing Internet Service Providers From Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 678 (2002).

115. Kim, *supra* note 2, at 398.

116. *See* Quist, *supra* note 94, at 287–88. In addition to the disagreement over the scope of the term publisher, circuit courts have split over whether "the defense established by § 230(c)(1) is properly understood as an 'immunity' defense." *See* Hare v. Richie, No. ELH-11-3488, 2012 WL 3773116, at *14 (D. Md. Aug. 29, 2012) (comparing Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010) and Almeida v. Amazon.com, Inc. 456 F.3d 1316, 1321 (11th Cir. 2006) with City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010) and Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100 (9th Cir. 2009)).

117. *See* Quist, *supra* note 94, at 287–88; Zeran v. Am. Online, Inc., 129 F.3d 327, 332–33 (4th Cir. 1997).

118. *See* Quist, *supra* note 94, at 287–89. The statute merely states that § 230(c) is a defense to liability. *See* 47 U.S.C. § 230(c). Yet the *Zeran* opinion "suggests that the grant of immunity is not only implied, but explicitly envisioned by the plain meaning of the language of Section 230(c)(1)." Quist, *supra* note 94, at 289.

Stratton decision and preclude publisher liability.[119] Thus, Congress's failure to include distributor liability in the language of § 230 demonstrates an intent to leave distributor liability as the only available form of ISP secondary liability.

Section 230 created an environment in which the ISP can hold dichotomous roles and use each classification to its advantage.[120] As one commentator observed, ISPs are able to "exploit inflexible and dichotomous regulatory classifications to qualify as both creators and managers of content, and as intentionally neutral conduits of content created by others. With nimble maneuvering, ISPs can toggle between claiming First Amendment-protected speaker rights and invoking 'safe harbor' exemptions from liability for the content they carry."[121] Section 230 immunity provides ISPs an unfair advantage, the ability to utilize the classification that best suits its needs to the injured party's detriment.[122]

Moreover, there are limited avenues for relief under § 230, making § 230's application and remedies in comparison to other laws governing the Internet.[123] For example, other federal statutes provide notice and takedown remedies while also protecting the ISPs from liability.[124] Finally, the absence of a takedown provision in § 230 effectively creates a wall of immunity around harmful speech. By immunizing ISPs from liability and from the equitable relief of an injunction, § 230 enables the defamatory statements to remain online even after they have been found defamatory, becoming a statutory shield for wrongful conduct. In this manner, the ISP becomes a vehicle for permanent dissemination of the defamatory content. Accordingly, an amendment is needed to update § 230 to address the Internet's landscape and growing dissatisfaction with the ambiguity of § 230(c) immunity.

---

119. *See* Cannon, *supra* note 65, at 63.

120. *See* Rob Frieden, *Invoking and Avoiding the First Amendment: How Internet Service Providers Leverage Their Status as Both Content Creators and Neutral Conduits*, 12 U. PA. J. CONST. L. 1279, 1281 (2010).

121. *Id.*

122. *See* Lipton, *Intermediated Information Exchange*, *supra* note 51, at 1355 (noting the need to refocus the cyberlaw field to create an effective framework for remedying the "facially disparate areas of law like intermediary liability for defamation.").

123. For example § 230 is inconsistent with 17 U.S.C. § 512, the Digital Millennium Copyright Act of 1998 (DMCA). *Compare* 47 U.S.C. § 230, *with* 17 U.S.C. § 512. The DMCA, which was drafted around the same time as the CDA, also includes a safe harbor from liability for ISPs provided the ISP complies with the notice and takedown provision of § 512(c). 17 U.S.C. § 512(c).

124. Under the DMCA, ISPs still receive protection from liability for user-generated content; however the DCMA provides victims of copyright infringement with sufficient avenues to remedy the infringement. *See* 17 U.S.C. § 512. In comparison, there are limited avenues for relief under § 230 for victims of cyber defamation.

IV. THE INTERNET, THE UNITED KINGDOM, AND DEFAMATION LAW

Examining the relationship between defamation law and the Internet in countries such as the United Kingdom is "of critical importance" to proposing an amendment to § 230 of the CDA because of the Internet's global scope.[125] Of particular interest to the United States is the newly passed U.K. Defamation Act 2013, which became effective January 2014. The Act was designed to amend the previous defamation statute and address several concerns that had arisen with the increase in popularity of the Internet. Before analyzing the Act, it is important to understand the interplay between the U.K. laws and the European Union Electronic Commerce Directive prior to the passage of the U.K. Defamation Act 2013.

A. *The 1996 U.K. Defamation Act and the European Union Electronic Commerce Directive*

In 1996, the same year Congress passed § 230 of the CDA, the United Kingdom codified the Defamation Act of 1996 (1996 U.K. Act).[126] The 1996 Act did not contain any provisions addressing the Internet or ISPs.[127] However, four years after the 1996 U.K. Act came into effect, the European Union set forth its Legislation Directive on Electronic Commerce.[128] The European Union's purpose in creating the Electronic Commerce Directive was "to remove obstacles to cross-border provision of on-line services in the Internal Market and to provide legal certainty to businesses and citizens."[129] To further this goal, Articles 12 to 14 of the Directive established "precisely defined limitations on the liability of intermediary service providers who offer mere conduit, caching and hosting."[130]

Specifically, Article 14(1) created a safe harbor provision from liability for ISPs.[131] Under the safe harbor provision, an ISP would be

125. GEORGE B. DELTA & JEFFREY H. MATSUURA, § 11.04 DEFAMATION AND THE INTERNET AROUND THE WORLD (3d ed. 2013).

126. Defamation Act, 1996, c. 31 (U.K.). Prior to the enactment of the 1996 U.K. Defamation Act, defamation law in the United Kingdom was defined solely by common law. *See* DELTA & MATSUURA, *supra* note 125, at 1.

127. Defamation Act, 1996, c. 31 (U.K.).

128. E.U. Electronic Commerce Directive, *supra* note 13. The European Union Electronic Commerce Directive contained numerous findings relating to ISPs, liability, and the Member States. *Id.* at 45, 46, 52, 64.

129. *Study on the Liability of Intermediaries*, at 4 (Nov. 12, 2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

130. *Id.*

131. Article 14(1) provides in pertinent part:

> 1. Where an information society service is provided that consists of the storage

immune from liability if the ISP complied with the notice-and-takedown requirements of the Directive.[132] This safe harbor provision and the 2000 E.U. Directive as a whole altered the application of laws governing ISP liability within each E.U. Member State, including the United Kingdom.[133] In 2012, the U.K. courts essentially adopted the safe harbor provisions of Article 14(1) in *Tamiz v. Google*, where the court held that Google could face potential liability as a publisher for failing to take down defamatory content after receiving notice that the content was defamatory.[134] The *Tamiz* decision changed the U.K. standard for ISP liability by deeming the ISP a publisher and subject to liability for allegedly defamatory content if "it fails to take action within a reasonable time after the complaining party notifies it."[135]

B. *The "New" U.K. Defamation Act of 2013*

The widespread growth of the Internet combined with the requirement to comply with the E.U. Directive culminated in the U.K. Parliament amending the 1996 U.K. Act.[136] In April 2013, the new U.K. Defamation Act of 2013 (2013 U.K. Act) passed by Royal Assent.[137] The 2013 U.K.

> of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

See E.U. Electronic Commerce Directive, *supra* note 12, art. 14(1).

132. *Id.*

133. *See id.* Because the E.U. Directive is a form of legislation governing its Member States, the Directive sets the floor for the laws in Member States. *Application of EU Law: Directives Definition*, (June 11, 2012), http://ec.europa.eu/eu_law/directives/directives_en.htm. The Member States are subsequently tasked with enacting or amending laws to remain in compliance with the Directive; however, the Directive is the minimum the Member States have to meet. *See* KLAUS-DIETER BORCHARDT, THE ABC OF EUROPEAN UNION LAW, 88–90 (Publ'n Office of the European Union 2010), *available at* http://europa.eu/documentation/legislation/pdf/oa8107147_en.pdf.

134. *See* Tamiz v. Google Inc., [2012] EWHC 449 (QB).

135. *Id.*; DELTA & MATSURA, *supra* note 125.[quote not found in article]

136. *See* Jennifer Agate, *The Defamation Act 2013 – Key Changes for Online*, C.T.L.R. 2013, 19(6), 170–71 (2014) [unable to find source] ("The Act also introduces two new defences for online publishers, a recognition of the unique nature of online publication and an apparent attempt to place more responsibility on the authors of web posts, a group who (with a few notable exceptions) have until recently been fairly confident of their untouchability.").

137. Defamation Act, 2013, c. 26 (U.K.).

Act's relevant changes to the existing defamation law include a tightening of the requirements for plaintiffs to prevail on a defamation claim and an incorporation of the E.U. Directive safe harbor provision.[138] Sections 5 and 13 of the 2013 U.K. Act are particularly relevant for U.S. proposals to amend § 230 of the CDA to address cyber misconduct.

Notably, the U.K. tailored the act to address cyber defamation by adding a section pertaining solely to website operators.[139] Section 5 of the 2013 U.K. Act, titled "Operators of Websites" is applicable when "an action for defamation is brought against the operator of a website in respect of a statement posted on the website."[140] Similar to the CDA, Section 5 provides website operators increased protection from defamation liability for user-generated content by creating a defense from liability.[141] Under Section 5, the website operator bears the burden of proving that the defamatory content was user-generated; and if the website operator meets this burden, then the website operator is entitled to a defense from liability.[142] However, the defense provided to website operators under Section 5 is a conditional defense and is "defeated" if the plaintiff proves that:

> (a) it was not possible for the claimant to identify the person who posted the statement,
> (b) the claimant gave the reporter a notice of complaint[143] in relation to the statement, and
> (c) the operator failed to respond to the notice of complaint in accordance with any provision contained in regulations.[144]

The United Kingdom further tailored the 2013 U.K. Act to address the unique problem of cyber defamation with Section 13 of the Act.[145] Section 13 provides courts with the authority to enforce a takedown decree for defamatory content against website operators.[146] Section 13(1) provides:

---

138. *See id.*; Corey Omer, *Intermediary Liability for Harmful Speech: Lessons From Abroad*, 28 HARV. J.L. & TECH. 289, 309 (2014) (noting that the "2013 Defamation Act clarified and made several significant changes to the law on intermediary liability for defamatory content in the U.K.").

139. *See* Defamation Act, 2013, c. 26, § 5 (U.K.).

140. Defamation Act, 2013, c. 26, § 5(1) (U.K.)

141. *See* Defamation Act, 2013, c. 26, § 5(2) (U.K.).

142. Defamation Act, 2013, c. 26, § 5 (U.K.).

143. Defamation Act, 2013, c. 26, § 5(3) (U.K.). Section 5(6) of the 2013 U.K. Act sets out what needs to be included in a notice of complaint. Defamation Act, 2013, c. 26, § 5(6) (U.K.).

144. Defamation Act, 2013, c. 26, § 5(3) (U.K.).

145. Defamation Act, 2013, c. 26, § 13 (U.K.).

146. *Id.*

> Where a court gives a judgment for the claimant in an action for defamation the court may order –
> (a) the operator of a website on which the defamatory statement is posted to remove the statement, or
> (b) any person who was not the author, editor or publisher of the defamatory statement to stop distributing, selling or exhibiting material containing the statement.[147]

Under Section 13, the court's authority to enforce a takedown decree against the website operator is not triggered until the court has entered a judgment in the plaintiff's favor by finding the content defamatory. Section 13 also enables the court to order the website operator to takedown defamatory content in situations where the author of the defamatory content "may not always be in a position to remove or prevent further dissemination of material which has been found to be defamatory."[148] Thus, Section 13 promotes efficiency in responding to and remedying the harm caused by the defamatory content because it enables courts to enter "an order for removal of the material to be made during or shortly after the conclusion of proceedings."[149]

C. *Potential Areas of Concern for the United States*

With its enactment, the 2013 U.K. Act brought renewed attention worldwide to amending laws governing cyber misconduct, specifically cyber defamation.[150] Although the 2013 U.K. Act has provided a framework for updating cyber laws, there are several sections of the 2013 U.K. Act that would prove problematic application in the United States.

First, although U.K. and U.S. defamation law are derived from the same base common law principles, each respective country places different weight and importance on the fundamental interests of free speech and reputation. In the United Kingdom, an individual's reputation interest is valued above the interests of free speech, whereas in the United States, free speech interests are valued above an individual's reputation interests.[151]

---

147. Defamation Act 2013, c. 26, § 13(1) (U.K.).

148. *See* comment 76 to Defamation Act 2013, c. 26, § 13 (U.K.).

149. *Id.*

150. The 2013 U.K. Act is a product of the concerted U.K. effort to update U.K. defamation law to properly account for the increased prevalence of the Internet as a modern day medium of communication. It has drawn attention to the account for the unique qualities and the pervasiveness of the Internet.

151. *See* DELTA & MATSURA, *supra* note 125. The differing emphasis placed on the free speech and reputation values has led the U.S. to view the U.K. defamation law as a mechanism for individuals to silence critics as opposed to protecting free speech and an open marketplace of

Additionally, under U.K. defamation law, the burden is placed on the defendant to prove the three elements of the defense to defamation.[152] In comparison, under U.S. common law defamation, the burden is placed on the plaintiff to prove that "the defendant was not an innocent disseminator."[153] Thus, where the 2013 U.K. Act does provide a defense for ISPs like § 230 does, the U.K. allocation of the burden of proof would not be well received in the United States.[154]

Finally, there is some ambiguity in the 2013 U.K. Act that needs clarification. Similar to the ambiguity in § 230 surrounding the meaning of the word "publisher,"[155] the 2013 U.K. Act does not define the term "website operator."[156] The failure to define website operator under the 2013 U.K. Act could create ambiguity as to whether any social media website or ISP could qualify for the conditional defense from liability pursuant to Section 5 of the Act.[157]

Despite the potential concern U.S. law and policy makers might have with the 2013 U.K. Act, there is one section, which adequately addresses the defamation victim's underlying goal of removing the defamatory material from the Internet. Section 13 of the 2013 U.K. Act provides the

---

ideas and discourse. *See* Sterling, *supra* note 18, at 338–40.

152. Defamation Act 2013, c. 26 (U.K.); *see* Sterling, *supra* note 18, at 338–40.

153. *See* DELTA & MATSURA, *supra* note 125, at 2.

154. In a similar vein, the Section 5 defense afforded website operators is conditioned upon the website operator identifying the third-party poster to the plaintiff pursuant to a notice request. *See* Defamation Act 2013, c. 26, § 5 (U.K.). Specifically, the website operator would have to provide the plaintiff "sufficient information to bring proceedings against the" unidentified third party poster. Defamation Act 2013, c. 26, § 5(4) (U.K.). This approach to providing a website operator defense from liability would not be feasible in the United States because it encourages website operators to disclose an unidentified poster's identity to the plaintiff. This would not only encroach on First Amendment interests, it could also have a chilling effect on free speech.

155. *Cf.* 47 U.S.C. § 230(c).

156. *See* Defamation Act 2013, c. 26, § 5 (U.K.); DELTA & MATSURA, *supra* note 125, at 9; Farrer & Co, *A Quick Guide to the Defamation Act 2013*, ENT. L.R. 2014, 25(2), 55–60 (2014).

> It is notable that key terms including "operators" and "posted on the website" are not satisfactorily defined, a situation not helped by the fact that the legislation uses relatively old-fashioned terms at a time when a lot of user generated content is nowadays published via mobile platforms and apps.

Id.

157. *See* Farrer & Co., *supra* note 156.

> It seems likely that there will be litigation over the scope of s.5. For example, will a website that temporarily suspends access to and later reinstates a post be determined to have posted the content? Further, who is the operator, the owner of the website, the ISP, the body with day to day control over its functions or two or more of these three?

Id.

courts with equitable power to enforce an injunction and takedown of the defamatory content following a judgment in plaintiff's favor after a trial on the merits.[158] It is this Section that Congress should focus on in drafting an amendment to § 230 of the CDA.

Moreover, if the United States creates a takedown notice provision then there will be a somewhat consistent application of this specific equitable remedy requirement for ISPs in the United States, United Kingdom, and E.U. Member States. This would be a positive step towards creating uniformity of laws and expectations pertaining to ISP liability in this multi-jurisdictional, global Internet.

V. PROPOSED SOLUTION: AMEND § 230 TO INCLUDE A FEDERAL TAKEDOWN REMEDY

As the use of the Internet as a primary medium of communication continues to grow, there is growing dissatisfaction with the safe harbor provision of § 230 of the CDA and the blanket immunity provided to ISPs from virtually all lawsuits.[159] With this growing dissatisfaction, legal scholars have recognized the need to amend § 230 to provide a takedown remedy for cyber defamation victims, yet no scholar has addressed the practicalities of implementing a federal takedown remedy for a state tort action. The CDA is the only federal statute that impedes the ability of victims of cyber misconduct to obtain an appropriate remedy. Thus, although other aspects of § 230 need to be updated, at a minimum § 230(c) needs to be amended to permit equitable relief such as a takedown remedy for victims of cyber misconduct, specifically cyber defamation. The solution this paper proposes would provide a practical mechanism for victims of cyber misconduct to enforce a takedown remedy against ISPs throughout all U.S. jurisdictions without subjecting ISPs to civil liability.

A. *Jurisdictional Concerns*

The crux of the problem facing proposed amendments to § 230 is that there is no federal defamation law. Absent a federal defamation law, challenges arise as to the enforcement of state court orders outside of the state, especially when the ISP is not a party to the lawsuit. The Supreme Court addressed this precise issue in *Baker by Thomas v. General Motors Corp.*[160]

158. Defamation Act 2013, c. 26, § 13 (U.K.).

159. *See, e.g.*, Kim, *supra* note 2; Horton, *supra* note 10; Quon, *supra* note 19; Jeweler, *supra* note 109.

160. Baker by Thomas v. Gen. Motors Corp., 522 U.S. 222 (1998).

In *Baker*, the Court was faced with determining whether an injunction issued in the state of Michigan should be recognized and enforced pursuant to the Full Faith and Credit Clause in other states.[161] The Court distinguished between the credit owed by states to judgments and to mechanisms for enforcing judgments.[162] It held that for judgments, "the full faith and credit obligation is exacting."[163] A "final judgment in one State, if rendered by a court with adjudicatory authority over the subject matter and persons governed by the judgment, qualifies for recognition throughout the land . . . [thus] the judgment of the rendering state gains nationwide force."[164]

Although a judgment against a party would be recognized throughout the nation pursuant to the Full Faith and Credit Clause, the Court acknowledged that the question of *enforcing* an injunction or other equitable decree was still unanswered. The Court noted that equity decrees still fall within the purview of the "full faith and credit domain."[165] However, the *enforcement* of a judgment or equitable decree does not have credit nationwide,[166] "such measures remain subject to the evenhanded control of forum law."[167] The Court concluded that the Michigan injunction would not have full faith and credit nationwide, because the Michigan court lacked authority to "command obedience" in other states against parties not subject to the Michigan lawsuit or to the jurisdiction of the court.[168]

If Congress amended § 230 to allow courts in cyber defamation claims to issue takedown decrees for ISPs after a finding in plaintiff's favor, the question then presented is how would a state court judgment and injunction be enforced against an ISP when the ISP is not party to the suit and potentially when the ISP is domiciled in a sister state? Justice Scalia's concurring opinion in *Baker* addressed this exact dilemma.[169] Justice Scalia noted that "[n]o execution can issue upon such judgments without

161. *Id.* at 226.

162. *Id.* at 232.

163. *Id.* at 232–33.

164. *Id.* at 233.

165. *Id.* at 234 ("Equity decrees for the payment of money have long been considered equivalent to judgments at law entitled to nationwide recognition.").

166. *See id.*

167. *Id.* at 235 ("Full faith and credit, however, does not mean that States must adopt the practices of other States regarding the time, manner, and mechanisms for enforcing judgments."); *see* McElmoyle *ex rel.* Bailey v. Cohen, 38 U.S. (13 Pet.) 312, 325 (1839).

168. *Id.* at 239–41 (citing Thomas v. Wash. Gas Light Co., 448 U.S. 261, 282–83 (1980) ("Full faith and credit must be given to [a] determination that [a State's tribunal] had the authority to make; but by a parity of reasoning, full faith and credit need not be given to determinations that it had no power to make.")).

169. *Id.* at 241–42 (Scalia, J., concurring).

a new suit in the tribunals of other States."[170] Further, Justice Scalia stated that for a state court judgment to be effective in a sister state, "it must be made a judgment there; and can only be executed in the latter as its laws may permit."[171]

Therefore, numerous jurisdiction and enforcement obstacles would arise when enforcing a state tort defamation judgment and subsequent injunctive takedown order in other states against ISPs not party to the underlying defamation action. Moreover, it would be tedious to create a statutory remedy that requires the successful plaintiff to go into each individual state court and domesticate the original court takedown order to have the other state courts enforce it.

B. *The Interplay Between the Full Faith and Credit Clause and the Full Faith and Credit Statute*

Before the solution this Article proposes can be fully understood and set out, it is important to understand how the interplay between the Full Faith and Credit Clause of the Constitution and 28 U.S.C. § 1738 the Full Faith and Credit Statute, factor into and assist the successful enforcement of a federal takedown remedy.

The Full Faith and Credit Clause, Article IV § 1 of the Constitution of the United States, provides that "Full Faith and Credit shall be given in each State to. . . . judicial Proceedings of every other State. And the Congress may by general Laws prescribe the Manner in which such . . . Proceedings shall be proved, and the Effect thereof."[172] In June of 1948, Congress used the authority granted to it under the Full Faith and Credit Clause to enact the Full Faith and Credit Statute.[173] The Full Faith and Credit Statute provides that:

> The records and judicial proceedings of any court of any such State, Territory or Possession, or copies thereof, . . . shall have the same full faith and credit in every court within the United States and its Territories and Possessions as they have by law or usage in the courts of such State, Territory or Possession from which they are taken.[174]

Congress established, *via* 28 U.S.C. § 1738, a federal statute

170. *Id.* (quoting Thompson v. Whitman, 85 U.S. (18 Wall.) 457, 462–63 (1873)).

171. *Id.* at 242 (quoting Lynde v. Lynde, 181 U.S. 183, 187 (1901)); *see* McElmoyle *ex rel.* Bailey at 325.

172. U.S. CONST. art. IV, § 1.

173. 28 U.S.C. § 1738 (2006).

174. *Id.*

mandating that judgments of state courts shall have nationwide force.[175] Therefore, a judgment issued by a state court will be recognized by state and by federal courts.[176]

When an issue reaches a federal court, the court is required to give the state judgment the same force and effect it has in the state in which it was rendered, including preclusive effect in any future proceeding or action.[177] While the courts are required to give the judgment full faith and credit, they are still not required to give full faith and credit to enforcement measures.[178] Thus, an equitable decree such as a takedown remedy is binding and enforceable throughout the United States, only if a federal court issues it.[179]

C. *Amend § 230 to Include a Federal Takedown Remedy Provision*

After examining the current state of Internet defamation law, Congress's goals behind § 230 of the CDA and the inequities victims of cyber misconduct face, the only practical solution is to amend § 230 to add a section creating a federal takedown remedy. This federal takedown remedy will not interfere with an ISP's protection from civil liability; instead, it will enable successful defamation plaintiffs[180] to enforce a takedown remedy in federal court against the ISPs.

There are two possible methods by which a Federal Takedown Remedy Provision could be added to § 230 of the CDA. The federal takedown remedy provision could be added as a new subpart of § 230(c) the Good Samaritan provision. However, adding the federal takedown remedy provision as a new subpart to § 230(c) would add more confusion to an already ambiguous provision. The second option, adding a completely new provision to § 230, would be the most practical method of adding a federal takedown remedy provision to the CDA. The creation of a new provision under § 230 would not only assist cyber defamation plaintiffs in achieving the true remedy they desire, takedown of the defamatory content, it also updates § 230 to account for the unique aspects of the Internet.

A full version of the proposed draft of the Federal Takedown Remedy Provision is attached as Appendix A. The major focus, aside from creating the ability to seek a takedown remedy, is ensuring that the

175. *Id.*

176. *Id.*

177. *See id.*

178. *See id.*

179. *See* 28 U.S.C. § 1738. An equitable decree issued by a federal court will not encounter the enforcement problem discussed in *Baker* for state court equitable decrees. Compare 28 U.S.C. § 1738, with Baker by Thomas, 522 U.S. at 239–41.

180. By successful defamation plaintiffs, I am referring to plaintiffs in situations where a judge has adjudicated the content defamatory.

takedown decree will have nationwide enforcement subject to federal jurisdiction. In adding a Federal Takedown Remedy to § 230 of the CDA, the majority of the statute would remain unchanged. The only change to the pre-existing language would be to § 230(c) to add a reference to the federal takedown remedy of § 230(g). This would incorporate the new provision so there would not be confusion as to whether § 230(c) or the new § 230(g) applied.

The new provision, the proposed federal takedown remedy of § 230(g) bestows jurisdiction upon the federal district courts to grant and enforce an injunction, a takedown decree, against an interactive computer service. Proposed § 230(g)(1) provides:

> (g)(1) Takedown Process: to qualify for the federal takedown remedy:
>
> (A) The plaintiff shall file a suit for defamation in the appropriate state court against the author or poster of the defamatory statement. No later than the third day after service of process on the author or poster, the plaintiff shall request the court to issue a Notice of Action and Right to Intervene to the interactive computer service.
>
> (i) The plaintiff's complaint shall include the following:
>
> (1) the identity and address of the interactive computer service;
> (2) a Notice of Action and Right to Intervene addressed to the interactive computer service;
> (3) reference the plaintiff's intent to file for the takedown remedy pursuant to this section of § 230 after the conclusion of a trial in plaintiff's favor; and
> (4) the plaintiff's request for a referral to the district court if the plaintiff prevails.
>
> (ii) The Notice of Action and Right to Intervene shall include the following:
>
> (1) a copy of the complaint;
> (2) a statement that plaintiff seeks to enforce a takedown decree pursuant to this section of § 230 after the conclusion of a trial in plaintiff's favor;
> (3) a statement that the interactive computer service has the right to intervene; and
> (4) inform the interactive computer service of a deadline to intervene which shall be no later than the 20th day after the date

that the interactive computer service is served with the notice of Action and Right to Intervene.

(iii) The Interactive Computer Service's Right to Intervene. If the interactive computer service elects to intervene, then the interactive computer service shall file a notice to intervene and a motion to remove the case to the appropriate district court pursuant to this statute.

(B) If the interactive computer service does not intervene, then the state court case proceeds without the interactive computer service as a party. If the plaintiff prevails and a judgment is entered in plaintiff's factor, then the plaintiff may qualify for the takedown remedy.

(C) If the plaintiff prevails, the plaintiff may register the state court judgment with the appropriate district court. The plaintiff shall file a motion in the district court requesting the court to recognize the state court judgment and issue a takedown decree directing the interactive computer service to takedown the defamatory statement(s) pursuant to this provision of § 230.

Under proposed § 230(g)(1)(a), the plaintiff is required to provide notice of intent to assert the federal takedown remedy pursuant to the statute or they may be precluded from qualifying for and enforcing the federal takedown remedy. With the notice and right to intervene aspect of § 230(g)(1)(A), if the interactive computer service (ISP) elects to intervene, then the matter will be removed to district court bringing the matter directly under federal jurisdiction. The next provision § 230(g)(1)(B) requires the plaintiff prevail on the state court defamation claim. This provision would ensure that a court has determined the speech is defamatory and thus no longer subject to First Amendment protection before the order of takedown. Then under § 230(g)(1)(C), if a plaintiff prevails, the plaintiff is able to register the judgment with the appropriate district court pursuant to the terms of this federal takedown statute. By registering the judgment, the state court judgment turns into a federal judgment and corresponding federal injunction, enforceable in the United States.

Proposed § 230(g)(2) provides the safe harbor provisions to provide ISPs with defenses from monetary liability in keeping with the overall spirit of § 230, it provides:

(g)(2) Safe Harbor: Defense to and Protection from Federal Takedown Remedy

> (A) If the interactive computer service permits users to delete and edit content after the user has posted the content on the website, then the interactive computer service is not subject to this provision of § 230 and is afforded the protection under § 230(c).
>
> (B) If the interactive computer service, upon receipt of Notice of Action and Right to Intervene from (1)(a), elects not to intervene, the interactive computer service may consent in writing to takedown the defamatory content should a judgment be entered in plaintiff's favor. If the interactive computer service files its written consent in the state court and takes down the defamatory content after it receives notice of a judgment in plaintiff's favor, then the interactive computer service is not subject to this provision of § 230 and is afforded the protection under § 230(c). If the interactive computer service fails to takedown the defamatory content, no later than the 20th day after notice of judgment is received, then the interactive computer services is not protected from the federal takedown remedy and the plaintiff may register the judgment with the appropriate district court.
>
> (C) This provision shall not subject an interactive computer service to monetary relief. However, if the interactive computer service fails to comply with a takedown decree pursuant to this section, the interactive computer service shall be held in contempt and subject to monetary sanctions.

Section 230(2)(A) provides that if the ISP enables its users to have editorial control, then the state court will be able to issue an injunction against the poster to have the defamatory content taken down. Further § 230(g)(2)(B), promotes efficiency by enabling the ISP to save costs by allowing them to provide notice of intent to comply in writing after they receive notice of a judgment in plaintiff's favor. The ISP will not have to intervene, and so long as they comply within the specified time, they will not be subject to the federal takedown and will be immune from liability. However, if the ISP fails to comply within the specified time period, then the plaintiff can proceed under the terms of the statute by registering the judgment in district court. Finally, § 230(g)(2)(C) includes a statement reiterating that the section only subjects ISPs to takedown decrees without opening the door for monetary liability. The only caveat is that if the ISP fails to comply with the federal injunction, it would be subject to the court's contempt power, which includes a monetary fine.

Instituting a federal takedown remedy in a manner similar to the one proposed above will ensure that a prevailing plaintiff is able to enforce a

judgment for cyber defamation against the ISP nationwide, even though the ISP might not be a party to the underlying defamation action.

D. *Potential Concerns with and Objections to Proposed Federal Takedown Remedy*

A federal takedown remedy such as the one proposed above might encounter opposition from interested parties such as ISPs. While there are several possible objections that may be presented, I will address each in turn and demonstrate how this solution nullifies such concerns.

First, as defamation is a state tort action, there are different standards for defamation in each state. Unless Congress enacts a federal defamation law, the standards will always differ to some extent, yet the foundation for each state defamation action is the same. As long as the victim is able to prove the content defamatory, the differing standards by state should not matter. Further, there could be concerns about added litigation costs for enforcing the takedown remedy pursuant to the statute. This concern could be easily remedied by placing the cost on the defendant of paying the fees to enact the takedown remedy.

Additionally, as the § 230 broad immunity has been consistently upheld since *Zeran*, the creation of a federal takedown remedy could be viewed as opening the doors for enforcing other causes of action against ISPs. However, the proposed addition to § 230 only permits the enforcement of the federal takedown remedy against ISPs and explicitly provides that ISPs are protected from all other civil liability.

The proposal and availability of a federal takedown remedy for Internet defamation action is a subject of controversy in the legal field. Most scholars in examining the remedies available in defamation cases have focused on the no-injunction rule and issues relating to prior restraint of speech in violation of the First Amendment.[181] However, "much of the current action in defamation cases," specifically cyber defamation, revolves around the issue of post-publication injunctions.[182] Generally, courts have consistently invoked the no-injunction rule in defamation cases.[183] Plaintiffs have been required to overcome the law's preference for legal over equitable remedies[184] and the First Amendment prior restraint doctrine.[185]

The First Amendment prior restraint doctrine also presents a sturdy

181. *See* Ardia, *supra* note 3, at 83; Rendleman *supra* note 20, at 4 ("A large grey area blurs the border between the background interests in reputation and expression.").

182. Ardia, *supra* note 3, at 83.

183. *Id.* at 20–21; *see* Rendleman *supra* note 20, at 5–6.

184. Ardia, *supra* note 3, at 32–34; Rendleman *supra* note 20, at 6 ("Maxim that 'Equity will not enjoin defamation.'").

185. Ardia, *supra* note 3, at 32–34; Rendleman *supra* note 20, at 6.

barrier to seeking an injunction in defamation cases.[186] In the seminal case of *Near v. Minnesota*, the Supreme Court first invoked the First Amendment's free speech guarantees to invalidate an injunction.[187] Following *Near*, courts utilized a case-by-case application of the prior restraint doctrine.[188] The Court first entertained the possibility of allowing an injunction in certain speech cases in *Pittsburgh Press Co. v. Pittsburgh Commission of Human Relations*.[189] The Supreme Court in *Pittsburgh Press* remarked that the concern with "prior restraint is that communication will be suppressed . . . before an adequate determination that it is unprotected by the First Amendment."[190] The Court left the door open for determining whether an injunction following a finding of defamation would be constitutional.[191]

Accordingly, there is an emerging trend "within both state and federal courts that permits injunctions if the speech in question was adjudged to be defamatory."[192] After examining the issue of injunctions in defamation cases, several scholars have concluded that injunctions may be permitted as a remedy to enjoin defamatory speech in certain contexts, such as when there has been an adjudication deeming the speech defamatory.[193] Thus, as proposed in the solution above, in the post-publication, post-adjudication context of Internet defamation, an injunction requiring the takedown of the defamatory content should not be barred by the First Amendment.[194] The proposed federal takedown remedy would be narrowly tailored and limited to post-publication speech found to be defamatory after a judgment on the merits.

Further, an interesting and somewhat novel concern could be the burden of a federal takedown remedy on ISPs. Here, requiring ISPs to remove defamatory content authored by a third party would not be unduly burdensome because ISPs are required to do this routinely in other countries.[195] There is one final characteristic of the proposed federal

186. *See* Ardia, *supra* note 3, at 32–33; Rendleman *supra* note 20, at 23.

187. Near v. Minnesota, 283 U.S. 697, 723 (1931) (invalidating an injunction because it "imposes an unconstitutional restraint upon publication" violating the First Amendment).

188. Ardia, *supra* note 3, at 33.

189. Pittsburgh Press Co. v. Pittsburgh Comm'n of Human Relations, 413 U.S. 376 (1973).

190. *Id.* at 390.

191. *See id.*; Ardia, *supra* note 3, at 41 (citing Tory v. Cochran, 544 U.S. at 738–39 ("the Tory Court left the door open by stating that an injunction 'may still be warranted,' if it were 'tailored to these changed circumstances'.")).

192. *See* Ardia, *supra* note 3, at 51.

193. *See* Rendleman, *supra* note 20, at 90 ("strong recent scholarship by Professor Ardia and Dean Chemerinsky supports a limited defamation injunction.").

194. *See* Ardia, *supra* note 3, at 58, 60, 62; Rendleman *supra* note 20, at 92 ("a judge should consider an injunction to be an appropriate remedy for a defendant's proved defamation.").

195. *See* Defamation Act 2013, c.26 (U.K.); E.U. Electronic Commerce Directive, *supra* note 12.

takedown remedy that is necessary to quell concern. The federal takedown remedy will only be enforceable in the United States, its territories and possessions. The federal takedown remedy will not address situations where the ISP is not domiciled in the United States and enforcement is difficult.[196] This will always be a problem regardless of changes to § 230 until there is a global Internet law with takedown remedies enforceable against all ISPs.

VI. CONCLUSION

Eighteen years have passed since Congress enacted the CDA with the goal of promoting the growth of the Internet.[197] Today, the Internet is a pervasive part of everyday life, and the CDA, specifically § 230, is no longer equipped to adequately address the legal problems that arise due to the unique aspects of the Internet. While U.S. scholars have remarked on the need to amend § 230 to include a takedown remedy, no scholar has considered the jurisdictional and practical problems of enforcing a federal takedown remedy for a state tort defamation claim.

The U.K. Defamation Act 2013 provides insight into methods for amending § 230 of the CDA to account for the problem of cyber defamation on the Internet. This Article, after studying the 2013 U.K. Act and both the jurisdictional and constitutional problems associated with cyber defamation in the United States, provides guidance for how to effectively amend § 230 of the CDA. The proposed solution in this Article will restore the inequities facing victims of cyber defamation to a proper balance. This solution sets forth a framework for amending § 230 to include a federal takedown remedy, which will be enforceable throughout all U.S. jurisdictions. While this solution will not address the problem of global cyber defamation, this solution will bring § 230 in line with similarly situated countries. Cyber defamation victims will be in a better position to seek and achieve the remedy they desire, takedown of the defamatory content. Although § 230 broad ISP immunity needs to be re-evaluated, a federal takedown remedy will remain crucial and necessary to maintaining a balanced and fundamentally fair legal system for cyber defamation victims in light of the unique aspects of the Internet.

196. Rendleman, *supra* note 20, at 56 ("The Internet is international. An injunction that forbids defendant's Internet defamation may not be effective because the injunction may be followed by copying and mirror sites, some overseas. Potential defendants may be beyond the court's jurisdiction over persons and territory.").

197. 47 U.S.C. § 230 (1998).

Appendix A: Proposed Draft of Federal Takedown Remedy Provision

230(c) Protection for "good samaritan" blocking and screening of offensive material

(2) Civil liability
No provider or user of an interactive computer service shall be held liable for monetary relief, or except as provided in subsection (g), for injunctive or other equitable relief,[1] 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).

(g) Proposed Federal Takedown Remedy: (new provision)[2]

(1) Takedown Process: To qualify for the federal takedown remedy:

(A) The plaintiff shall file a suit for defamation in the appropriate state court against the author or poster of the defamatory statement. No later than the third day after service of process on the author or poster, the plaintiff shall request the court to issue a Notice of Action and Right to Intervene to the interactive computer service.

(i) The plaintiff's complaint shall include the following:

(1) the identity and address of the interactive computer service;
(2) a Notice of Action and Right to Intervene addressed to the interactive computer service;
(3) reference the plaintiff's intent to file for the takedown

[1] This added language comes from the language of the notice-and-takedown provision of the DMCA. 17 U.S.C. § 512(c).
[2] This provision bestows jurisdiction upon the federal district courts to grant and enforce an injunction, a takedown decree, against an interactive computer service.

remedy pursuant to this section of § 230 after the conclusion of a trial in plaintiff's favor; and
(4) the plaintiff's request for a referral to the district court if the plaintiff prevails.

(ii) The Notice of Action and Right to Intervene shall include the following:

(1) a copy of the complaint;
(2) a statement that plaintiff seeks to enforce a takedown decree pursuant to this section of § 230 after the conclusion of a trial in plaintiff's favor;
(3) a statement that the interactive computer service has the right to intervene; and
(4) inform the interactive computer service of a deadline to intervene which shall be no later than the 20th day after the date that the interactive computer service is served with the Notice of Action and Right to Intervene.

(iii) The Interactive Computer Service's Right to Intervene

If the interactive computer service elects to intervene, then the interactive computer service shall file a notice to intervene and a motion to remove the case to the appropriate district court pursuant to this statute.

(B) If the interactive computer service does not intervene, then the state court case proceeds without the interactive computer service as a party. If the plaintiff prevails and a judgment is entered in plaintiff's favor, then the plaintiff may qualify for the takedown remedy.

(C) If the plaintiff prevails, the plaintiff may register the state court judgment with the appropriate district court. The plaintiff shall file a motion in the district court requesting the court to recognize the state court judgment and issue a takedown decree directing the interactive computer service to takedown the defamatory statement(s) pursuant to this provision of § 230.

(2) Safe Harbor: Defense to and Protection from Federal Takedown Remedy

(A) If the interactive computer service permits users to delete and

edit content after the user has posted the content on the website, then the interactive computer service is not subject to this provision of § 230 and is afforded the protection under § 230(c).

(B) If the interactive computer service, upon receipt of Notice of Action and Right to Intervene from (1)(a), elects not to intervene, the interactive computer service may consent in writing to takedown the defamatory content should a judgment be entered in plaintiff's favor. If the interactive computer service files its written consent in the state court and takes down the defamatory content after it receives notice of a judgment in plaintiff's favor, then the interactive computer service is not subject to this provision of § 230 and is afforded the protection under § 230(c). If the interactive computer service fails to takedown the defamatory content, no later than the 20th day after notice of judgment is received, then the interactive computer service is not protected from the federal takedown remedy and the plaintiff may register the judgment with the appropriate district court.

(C) This provision shall not subject an interactive computer service to monetary relief. However, if the interactive computer service fails to comply with a takedown decree pursuant to this section, the interactive computer service shall be held in contempt and subject to monetary sanctions.

Florida Journal of International Law

VOLUME 27 | DECEMBER 2015 | NUMBER 3

STATEMENT OF PURPOSE

The *Florida Journal of International Law* is a scholarly publication devoted to timely discussion of international legal issues. Its subscribers include legal scholars and practitioners from around the world. The *Journal* publishes three times a year and is one of four co-curricular journals produced at the University of Florida Fredric G. Levin College of Law. On occasion, the *Journal* will also have Special Editions that can be purchased in addition to its subscription.

The *Journal* selects its editorial board and staff from the top ten percent of students at the University of Florida Fredric G. Levin College of Law and from winners of the open write-on competition held once per year.

The *Journal* enables students to earn academic credit while honing their legal research and writing skills. Recent articles published or accepted for publication have treated subjects as varied as International Trade and Commerce law, Human Rights law, Terrorism, National Security, War Crimes Tribunals, International Environmental law, International Intellectual Property, and Maritime law.

Florida Journal of International Law

The *Florida Journal of International Law* (ISSN 1556-2670) is a student-edited legal journal published by the University of Florida. The *Journal* is published three times per year. The *Journal* extends its deep appreciation for the generosity of the University of Florida Fredric G. Levin College of Law in supporting and assisting the *Journal* in its publication of this issue.

Editorial and business address: *Florida Journal of International Law*, University of Florida Levin College of Law, 351 Village Dr., 218 Bruton-Geer Hall, P.O. Box 117635, Gainesville, FL 32611.

Please visit us on the web at www.fjil.org/.

The subscription rate per volume is $55.00 U.S. domestic plus sales tax for Florida residents and $60.00 U.S. international. Single issues are available for $20.00 U.S. domestic and $25.00 U.S. international.

Back numbers (volumes 1-26 inclusive) are available from: William S. Hein & Co., 1285 Main Street, Buffalo, NY 14209.

Manuscripts may be submitted to the Articles Editors:

Florida Journal of International Law
Levin College of Law
University of Florida
351 Village Drive
218 Bruton-Geer Hall
Gainesville, FL 32611
USA

(352) 273-0906

Printed by Western Newspaper Publishing Co., 537 East Ohio St., Indianapolis, IN 46204