Social Media Terror: Reevaluating Intermediary Liability 
Under the Communications Decency Act

“The Internet has grown up, why hasn’t the law?”¹

I. INTRODUCTION

Recently, family members of victims of terror attacks filed a series of lawsuits against social media companies such as Twitter, Facebook, and Google.² In Fields v. Twitter,³ the widow of an American killed in Amman, Jordan, sued Twitter for providing “material support” to the Islamic State of Iraq and Syria (ISIS) by “knowingly and recklessly provid[ing] ISIS with accounts on its social network.”⁴ Following Fields, in Gonzalez v. Google, Inc.,⁵ the family of a woman killed in the November 2015 terrorist attack in Paris sued Google for “knowingly permit[ting] terrorist group ISIS to use their social networks,” and enabling them to carry out various terror attacks.⁶ These lawsuits bring to the forefront new issues surrounding intermediary liability, and raise the important question of whether social media companies should be liable, as intermediaries, for the illegal actions of their users.⁷


3. 217 F. Supp. 3d 1116 (N.D. Cal.), aff’d, No. 16-17165, 2018 WL 626800 (9th Cir. 2018).

4. Id. at 1119 (describing Twitter’s liability for facilitating terror attacks which killed plaintiff’s husband).


6. See Verified Complaint at 1-2, Gonzalez v. Twitter, Inc., No. 4:16-cv-03282 (N.D. Cal. June 14, 2016). Plaintiff Gonzalez initially filed suit against Twitter, Facebook, and Google, but has since amended the complaint and voluntarily dismissed the claims against both Twitter and Facebook. See id. (explaining cause of action against Twitter, Facebook, and Google); see also Gonzalez Complaint, supra note 2, at 1 (limiting action to Google).

7. See Joseph Monaghan, Note, Social Networking Websites’ Liability for User Illegality, 21 SETON HALL J. SPORTS & ENT. L. 499, 513-16 (2011) (questioning whether to impose liability on social media sites for users’ criminal acts); Should Twitter, Facebook Be Liable for a Terrorist Attack?, CBS (July 24, 2015), http://sanfrancisco.cbslocal.com/2015/07/24/should-twitter-facebook-be-held-liable-for-a-terrorist-attack/ [https
Technological advances have improved the modern-day terrorist organization’s ability to plan and coordinate far more devastating attacks, making them more sophisticated than their predecessors. Social networking sites are known for their ability to bring like-minded people together, and terrorist organizations utilize these sites to recruit, fundraise, and spread terrorist propaganda. These websites create a convenient and inexpensive platform for terrorist organizations to expand their global reach, amass support

---


from other like-minded extremists, and capitalize on a larger network of diverse
talents and skills. Social media websites play an integral role in terrorist
operations, and efforts to cripple the terrorist threat online require these
companies to “take responsibility for the global implications of their platform”
by proactively monitoring and policing content.

When Congress passed the Communications Decency Act (CDA) in 1996,
the Internet was a relatively new phenomenon. Congress enacted the law
intending to foster the growth and development of the Internet by minimizing
governmental regulation and empowering Internet companies to monitor and
screen for objectionable content without the constant fear of incurring
liability. Nevertheless, in light of today’s technological advances, the
legislative objectives that § 230 once served are at risk of becoming obsolete.

10. See Counterterrorism Hearing, supra note 9, at 14 (statement of Brian Michael Jenkins, Senior
Advisor to the President) (emphasizing Internet pivotal to terrorist organizations); Raphael Cohen-Almagor,
The Role of Internet Intermediaries in Tackling Terrorism Online, 86 FORDHAM L. REV. 425, 428 (2017)
(rationalizing modern terrorism’s heavy reliance on Internet due to many shared functional features); Alexander
Tsesis, Social Media Accountability for Terrorist Propaganda, 86 FORDHAM L. REV. 605, 608-09 (2017)
(proclaiming social media websites indispensable to terrorists’ efforts to expand their expressive reach); see
also J.M. Berger & Jonathon Morgan, The ISIS Twitter Census: Defining and Describing the Population of
ISIS Supporters on Twitter 1, 2 (The Brookings Project on U.S. Relations With the Islamic World, Analysis
Paper No. 20, 2015) (researching ISIS Twitter habits and identifying number of known ISIS accounts). The
Brookings Institute’s report on the social media habits of ISIS shows that from September 2014 through
December 2014, there were at least 46,000 Twitter accounts belonging to ISIS supporters. See Berger &
Morgan, supra, at 2; see also Yasmin Merchant, How ISIS Recruits Through Social Media, FORDHAM POL.
cce/W7KU-G2TR] (detailing terrorists’ utilization of social media tools to recruit).

11. See Radicalization: Social Media and the Rise of Terrorism: Hearing Before the Subcomm. on Nat’l
Sec. of the H. Comm. on Oversight and Gov’t Reform, 114th Cong. 7 (2015) [hereinafter Radicalization
Hearing] (statement of Mark D. Wallace, Ambassador, United Nations) (stressing importance of social media
websites’ cooperation in efforts to combat terrorism); Counterterrorism Hearing, supra note 9, at 12 (statement
of Andrew Aaron Weisburd, Director, Society for Internet Res.) (contending social media companies can and
should do more to inhibit online terrorist activities); Susan Klein & Crystal Flinn, Social Media Compliance
Programs and the War Against Terrorism, 8 HARV. NAT’L SECURITY J. 53, 56-57 (2017) (recommending
legally requiring social media companies to institute compliance programs to monitor for terrorist activity); see
also Press Release, Senator Dianne Feinstein, Bill Would Require Tech Companies to Report Online Terrorist
Activity (Dec. 8, 2015), http://www.feinstein.senate.gov/public/index.cfm/2015/12/bill-would-require-tech-
companies-to-report-online-terrorist-activity [https://perma.cc/A9v4-GK7V] (focusing on ability of social
media companies to help prevent terrorism). The proposed bill requiring social media companies to report
terrorist activities would be modeled after the Protect Our Children Act of 2008. See Press Release, Senator
Dianne Feinstein, supra; see also 18 U.S.C. § 2258A (2012) (setting forth reporting requirements for various
online service providers).

Internet platform); JOEL R. REIDENBERG ET AL., SECTION 230 OF THE COMMUNICATIONS DECENCY ACT: A
SURVEY OF THE LITERATURE AND REFORM PROPOSALS 4, 6 (2012) (explaining how novelty of Internet during
1990s motivated passage of § 230); see also Andrew P. Bolson, Flawed But Fixable: Section 230 of the
Communications Decency Act at 20, 42 RUTGERS COMPUTER & TECH. L.J. 1, 1-2 (2016) [hereinafter Bolson
II] (commenting on evolution of Internet since enactment of § 230).


14. See Bolson I, supra note 1 (criticizing § 230 for being outdated and irrelevant); see also Kai Jia, Blog,
From Immunity to Regulation: Turning Point of Internet Intermediary Regulatory Agenda, J.L. & TECH. TEX.
The changing nature of the Internet demands action, and Congress has failed in this regard.15

This Note refutes the idea that Internet companies require unbridled immunity to survive, and suggests that legislative reform is needed to address the myriad of ways the Internet has changed since Congress enacted the CDA.16 Part II of this Note begins with the historical foundation of § 230 of the CDA before articulating the judicial development of § 230 through case law.17 Part II of this Note also illustrates how § 230 presents a major obstacle to plaintiffs seeking civil remedies under the Antiterrorism Act (ATA) by examining the historical underpinnings of the civil remedy provision of the ATA and its relation to § 230.18 Finally, in Part III, this Note concludes with recommendations for legislative reform and examines how these recommendations may address the flaws inherent in § 230.19

[15. See Bolson II, supra note 12, at 1-2 (imploring law to reflect changes in Internet technology); Bolson I, supra note 1 (lamenting congressional failure in responding to evolution of Internet). Congress’s failure to amend the CDA leaves victims of terrorism with a right but no remedy. See infra Section II.C (demonstrating insurmountable challenge CDA poses for victims of terrorism); see also Marbury v. Madison, 5 U.S. (1 Cranch) 137, 163 (1803) (emphasizing importance of furnishing legal remedy for violation of legal right).

16. See Counterterrorism Hearing, supra note 9, at 32 (statement of Evan F. Kohlman) (advocating for congressional action to incentivize social media companies to aid in antiterrorism efforts); REIDENBERG ET AL., supra note 12, at 46-49 (identifying areas undergoing legislative reform which implicate § 230); see also Patricia Spiccia, Note, The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given, 48 VAL. U. L. REV. 369, 410-13 (2013) (proposing ways in which CDA can be improved upon); Doug Lichtman & Eric Posner, Holding Internet Service Providers Accountable 5 (Univ. of Chi. L. School, John M. Olin L. & Econ., Working Paper No. 217, 2004) (arguing for need to bring Internet service providers into chain of responsibility). An Internet service provider (ISP) is defined as: “A business or other organization that offers Internet access, typically for a fee.” Internet Service Provider, BLACK’S LAW DICTIONARY (10th ed. 2014).

17. See infra Sections II.A.2-4 (providing historical foundation for § 230 and judicial development after enactment).


19. See infra Part III (recommending legislative reform to improve and revise § 230).
II. HISTORY

A. General History and Background of the CDA

1. Common Law Prior to Section 230

Prior to Congress’s enactment of § 230, common law principles dictated ISP liability for alleged defamatory content posted by its users. The common law liability scheme consisted of three categories: primary publishers, distributors, and conduits. Primary publishers, like magazines and newspapers, publicize defamatory material created by others; distributors are the newsvendors, bookstores, and libraries that disseminate the publications; and conduits such as service providers and phone companies merely provide the means of communication. Given the varying levels of involvement, the law imposed different standards of liability on offenders, depending on the category into which they fell. Under common law, primary publishers were held to the same standard of liability as original authors because they were in the best position to monitor and control content, and as a result, could have easily avoided or mitigated the harm caused by defamation. On the other hand, a distributor is liable for the distribution of a defamatory publication only if the distributor had actual or imputed knowledge of the defamation and failed to remove the defamatory post. Distributor liability hinged on the idea that even though distributors were not in a position to monitor and control content, they had the ability to minimize the harm of the defamation by refusing to sell or stock defamatory materials. Finally, even though common sense dictates


22. See id. at 588-590 (providing examples of publishers, distributors, and conduits).

23. See id. at 588 (assigning different standard of liability to various entities).

24. See Cianci v. New Times Publ’g Co., 639 F.2d 54, 60-61 (2d Cir. 1980) (reiterating well-recognized common law principle of publisher standard of liability). The defendant in Cianci was a newspaper that published several libelous statements accusing the plaintiff, a public official, of rape. See id. at 56. The Cianci court held that the defendant could not defensively claim that the statements were in fact uttered by the original publisher because under the republication rule, “one who republishes a libel is subject to liability just as if he had published it originally, [regardless of whether] he attributes the libelous statement to the original publisher.” See id. at 60-61; RESTATMENT (SECOND) OF TORTS § 578 (AM. LAW. INST. 1977) (detailing publisher liability); see also Freiwald, supra note 21, at 588 (recognizing primary publisher’s duty to mitigate harm caused by defamatory content).


26. See Freiwald, supra note 21, at 590 (reasoning heightened showing of fault required for distributor liability). It was not in the normal course of the distributing business to review content, and, therefore,
that conduits, such as a telephone company, would be the but-for cause of the transmission of the offensive content, defamation claims against those who merely provide communication services to others are too attenuated to warrant imposing liability.27

The novel and inchoate nature of the Internet in the early 1990s made it difficult for courts to distinguish ISPs under the traditional publisher-distributor framework.28 Some courts applied the distributor standard for liability to ISPs because they viewed them as similar to bookstores and libraries; other courts found ISPs to have more editorial control than distributors, and thus, applied the publisher standard for liability.29 As one court insightfully noted, "more ideas and information are shared on the Internet than any other medium. But when we try to pin down this medium of exchange, we realize how slippery our notion of the Internet really is."30 The struggle courts faced in applying the traditional framework to ISPs became apparent when Stratton Oakmont, Inc. v. Prodigy Services Co.,31 and Cubby, Inc. v. CompuServe, Inc.,32 resulted in conflicting decisions.33

In Cubby, a federal court used the distributor standard of liability to assess CompuServe’s liability regarding defamatory content posted on its journalism forum.34 The court regarded CompuServe as a distributor, who therefore could not be held liable for defamatory statements unless it knew or had reason to

distributors were not obligated to screen content to determine whether a particular publication might be offensive or defamatory. See id.

27. See id. at 589 (noting defamation claims against conduits too weak to successfully impose liability). More significantly, telephone companies have little, if any, opportunity to stop the offending content as they are obligated to serve all their paying customers. See id.

28. See Reidenberg et al., supra note 12, at 4; see also Blumenthal v. Drudge, 992 F. Supp. 44, 48 n.7 (D.D.C. 1998) (drawing attention to inherent differences between traditional forms of communication and communication on Internet platform). Stressing the unique ways communication takes place on the Internet, the Blumenthal court identified three differences between the Internet and traditional forms of communication: the Internet’s ability to maintain information sources is limitless; the distribution of information on the Internet is often unregulated; and the users and producers of Internet information are often the same people. See Blumenthal, 992 F. Supp. at 48 n.7; see also Anthony Ciolli, Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas, 63 U. Miami L. Rev. 137, 137-38 (2008) (highlighting Internet’s transformation).

29. See Reidenberg et al., supra note 12, at 4; infra notes 33-42 and accompanying text (observing courts struggle to apply publisher-distributor framework to online entities).

30. Blumenthal, 992 F. Supp. at 48 n.7 (noting challenges posed by unique nature of Internet).


33. Compare id. at 140-41 (applying distributor standard of liability because CompuServe lacked editorial control over publications), with Stratton Oakmont, 1995 WL 323710, at *4-5 (attributing publisher liability because Prodigy actively screened and filtered content).

34. See Cubby, 776 F. Supp. at 140-41.
know of the defamatory nature of those statements. The court analogized CompuServe to distributors like bookstores and newsvendors because it had minimal editorial control over its publications. The court determined that, similar to these other entities, it would be unreasonable to make CompuServe examine every publication for potentially defamatory statements.

In Stratton Oakmont, a New York state court departed from the Cubby decision and used the publisher standard of liability to assess Prodigy’s liability for third-party statements posted on its “internet bulletin board.” The court distinguished this case from Cubby for two main reasons. First, the defendant-business, Prodigy, represented itself to the public as having editorial control over the content posted on its bulletin boards. Second, and more importantly, Prodigy exercised control over the content by utilizing an automatic software screening program, which assisted employees in removing content that they deemed contrary to their business policy guidelines. Consequently, the court found itself “compelled to conclude . . . [that] P[rodigy] [was] a publisher rather than a distributor” because of the amount of editorial control Prodigy had in determining what members posted on its bulletin board.

2. The Legislative Response

The conflicting decisions in Stratton and Cubby created a paradoxical situation where ISPs that tried, but were unsuccessful, in removing all harmful statements.
material risked publisher liability, while ISPs that made no attempt to filter offensive material from their networks remained free from liability. 43 In particular, members of Congress and online intermediaries alike fretted over this nonsensical “rule” that would result in one of two extremes. 44 First, the fear of being subject to litigation would strongly discourage intermediaries from filtering content, thus increasing the amount of inappropriate content on the Internet. 45 At the other extreme, intermediaries might overcensor content and chill free speech on the Internet. 46 Ultimately, the illogicality of imposing a higher standard of liability on ISPs that made good faith attempts to screen for offensive material sparked legislative reform. 47

Motivated by the Stratton decision and concerns about the increased access to pornography and indecency on the Internet, Congress proposed several amendments to address the shortcomings of the common law regulation of the Internet. 48 Hoping to provide greater protections for children, Senator J. James Exon spearheaded the initial draft of the legislation. 49 His initial proposal amended § 223 of the Telecommunications Act and extended the “antiharassment, indecency, and antiobscenity restrictions” from phone calls to telecommunications devices and ISPs. 50 Members of the Internet technology industry strongly opposed Senator Exon’s attempt to regulate offensive content because such regulation would increase the burden of monitoring and filtering content, exposing them to greater liability. 51

Responding to the criticism of his proposal, Senator Exon added two new defenses to the CDA. 52 First, the “access provider” defense exempted from liability those entities that merely served as a means of access or connection to

44. See Cannon, supra note 43, at 62 (highlighting concerns over Stratton decision).
45. See Ciolli, supra note 28, at 148 (identifying one of two potential extremes resulting from Stratton decision).
46. See id. (discussing potential for speech chilling from Stratton decision).
47. See Reidenberg et al., supra note 12, at 5-6 (effectuating legislative reform and willingness to impose limited regulation of internet).
48. See id. at 6 (describing first steps to legislative reform).
49. See id. (outlining Senator Exon’s motivation behind initial CDA draft); Cannon, supra note 43, at 53 (highlighting Senator Exon’s concern about online pornography). The proliferation of pornography online and the relative ease of access that American youth have to it motivated Senator Exon’s initial CDA proposal. See Cannon, supra note 43, at 53. According to Senator Exon: “[T]he information superhighway should not become a red light district. This legislation will keep that from happening and extend the standards of decency which have protected telephone users to new telecommunications devices.” 141 Cong. Rec. 3203 (1995) (statement of Sen. Exon).
50. See Cannon, supra note 43, at 57-58, 92 (detailing proposed changes to Telecommunications Act).
51. See id. at 59 (noting original CDA’s lack of defenses and difficult position of ISPs); see also Reidenberg et al., supra note 12, at 6.
the Internet. Second, the “good faith” defense eliminated liability for entities that made reasonable efforts to restrict access to offensive materials. Specifically, the good faith defense represented a congressional response to the absurdity of the Stratton decision, as well as an attempt to protect intermediaries from being forced to choose between censoring content and risking liability, or doing nothing at all. These changes proved to be persuasive; on June 14, 1995, the Senate ratified the Exon Amendment.

Rejecting the notion that the federal government should regulate the Internet, Representatives Chris Cox and Ron Wyden introduced the Family Empowerment Amendment (FEA) on June 30, 1995, to preserve the technological integrity of the Internet. Unlike Senator Exon’s version of the CDA, the FEA took a more hands-off approach to the regulation of online content. Rather than increase federal regulation of Internet content, the FEA recognized that parents were better situated to protect their children by controlling their Internet access. Moreover, to encourage self-regulation amongst ISPs, the FEA included a “Good Samaritan” provision that protected ISPs who made good faith efforts to monitor and restrict offensive material from liability. Under the Good Samaritan provision, “[n]o provider or user of interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” In addition, the FEA protects ISPs who merely provide “information content providers” with the technical tools designed to restrict access to offensive

53. See id. at 59-60 (specifying details of “access provider” defense).
54. See id. at 60-61 (describing good faith defense).
57. See id. at 67, 67 n.78 (rejecting increased federal Internet regulation proposed by U.S. House of Representatives).
58. See Reidenberg et al., supra note 12, at 7 (differentiating FEA from Senator Exon’s version of CDA).
60. See Reidenberg et al., supra note 12, at 7 (acknowledging deference to private technology companies based on expertise and capabilities).
The House passed the FEA with an almost unanimous vote, providing the foundation for § 230. Congress passed the CDA on February 1, 1996, which included the amendments to § 223, and also codified the Good Samaritan provision contained in the FEA at 47 U.S.C. § 230. In particular, Congress enacted § 230 to overrule the Stratton decision and address the remaining deficiencies in the publisher-distributor framework as applied to ISPs. To help accomplish this goal, 47 U.S.C. § 230(f) makes the distinction between entities that are “information content provider[s]” as opposed to entities that are “interactive computer service[s].” Ultimately, after the Supreme Court’s ruling in Reno v. ACLU, only § 230 remains intact.

62. See REIDENBERG ET AL., supra note 12, at 7 (recognizing FEA protection of ISPs providing tools to facilitate censoring); see also infra note 76 and accompanying text (defining “information content provider” and providing case law examples).


64. See REIDENBERG ET AL., supra note 12, at 8 (noting Good Samaritan provision’s codification and amendments to § 223).

65. See id. (articulating deficiencies in common law standard of liability CDA intended to address). In enacting the CDA, Congress wanted to encourage the use of “blocking and filtering technologies” to restrict children’s access to objectionable online material, and to avoid chilling free Internet speech by imposing liability on intermediaries. See 47 U.S.C. § 230(b)(4); Joey Ou, Note, The Overexpansion of the Communications Decency Act Safe Harbor, 35 HASTINGS COMM. & ENT. L.J. 455, 458 (2013) (advancing congressional intent behind CDA). Thus, while the transmission of obscene, indecent, or offensive material to minors is illegal under the current version of § 223, § 230 provides some measure of protection for ISPs that attempt to restrict access. See 47 U.S.C. § 230(c); 47 U.S.C. § 223(a) (2012); Ou, supra, at 458 (illustrating how § 230 complements § 223 of CDA to protect ISPs and minors).

66. See 47 U.S.C. § 230(o)(2)(c) (providing statutory definition for “information content provider” and “interactive computer service”); see also infra notes 75-76 and accompanying text (distinguishing between information content provider and interactive computer service).


68. See id. at 882 (holding prior version of § 223 unconstitutional). After Congress passed § 223 in 1996, the American Civil Liberties Union sought declaratory judgment that the CDA was unconstitutional under the First and Fifth Amendments to the U.S. Constitution. See id. at 861-62. Designed to protect minors from unsavory Internet materials, the former § 223 criminalized the intentional transmission of “obscene or indecent” messages to minors (i.e., anyone under eighteen-years-old) and materials that “depict[ed] or describe[d]” “sexual or excretory . . . organs” in a way that the community would find “offensive.” See id. at 859-60. The Court held that § 223 violated the First Amendment because it was overly broad, and was essentially a content-based blanket restriction on all speech. See id. at 882. Section 223’s all-encompassing prohibitions would likely have chilled free speech because it criminalized both protected and unprotected speech. See id. at 872, 877. Furthermore, § 223’s failure to provide clear definitions and limit its application to its stated objectives made the law ambiguous and difficult to apply. See id. at 877-78. Ultimately, the Court declined to address the Fifth Amendment issues and concluded that § 223 of the CDA was unconstitutional because it “place[d] an unacceptably heavy burden on protected speech, and that the defenses” contained in it were insufficient to salvage an otherwise invalid and unconstitutional provision. See id. at 864, 882.
3. Language and Purpose of Section 230

From a broad perspective, Congress’s intent in enacting the CDA was clearly twofold: to remove the disincentives associated with screening and policing objectionable content, and to promote the free exchange of words and ideas on the Internet. From a broad perspective, Congress’s intent in enacting the CDA was clearly twofold: to remove the disincentives associated with screening and policing objectionable content, and to promote the free exchange of words and ideas on the Internet.69 Section 230(c) outlines the protections afforded to ISPs for the “‘Good Samaritan’ blocking and screening of offensive material.”70 Subsection (c)(1) evidences a congressional attempt to address the confusion courts had regarding ISP liability and the desire to overturn the Stratton decision.71 Subsection (c)(2) eliminates the threat of civil liability for ISPs that edit their posts in good faith, and appears targeted to encourage the use of filtering and editing technologies among ISPs.72 Though immunity under § 230 may appear scopic, in reality, its applicability is limited to only bar causes of action that seek to impose liability on ISPs in their capacity as intermediaries.73

Furthermore, the statute, in § 230(f)(2) and § 230(f)(3), defines and distinguishes between an “interactive computer service” and “information content provider” for liability purposes.74 An interactive computer service

70. 47 U.S.C. § 230(c) (providing Good Samaritan provision); cf. 17 U.S.C. § 512(c)(1)(A)(i)-(iii) (2012) (delineating Digital Millennium Copyright Act’s (DMCA) notice and take down provision). Similar to the Good Samaritan provision contained in the CDA, the DMCA provision states that service providers are immune from liability for copyright infringing material provided by third parties if the provider is not aware of the facts and circumstances surrounding the infringement in general. See 17 U.S.C. § 512(c)(1)(A)(i)-(iii). Nevertheless, subsection (c)(1)(A)(iii) departs from the approach taken in the CDA, as it requires the ISP, “upon obtaining such knowledge or awareness [to] [act] expeditiously to remove, or disable access to, the material.” See 17 U.S.C. § 512(c)(1)(A)(iii); see also Ryan Gerdes, Note, Scaling Back §230 Immunity: Why the Communications Decency Act Should Take a Page from the Digital Millennium Copyright Act’s Service Provider Immunity Playbook, 60 DRAKE L. REV. 653, 670 (articulating “red flag” test under DMCA safe harbor provision). Under the red flag test, immunity extends to service providers if they knew or should have known of the infringing activity, and failed to take down the infringing content. See Gerdes, supra, at 670; see also Michelle Rotter, Note, With Great Power Comes Great Responsibility: Imposing A “Duty to Take Down” Terrorist Incitement on Social Media, 45 HOFSTRA L. REV. 1379, 1405-06 (2017) (recommending imposing obligation on social media companies to remove terrorist incitement posts). But see ELECT. FRONTIER FOUND., THE IMPACT OF TRADE AGREEMENTS ON INNOVATION, FREEDOM OF EXPRESSION AND PRIVACY: INTERNET SERVICE PROVIDERS’ SAFE HARBORS AND LIABILITY 3-5, https://www.eff.org/files/filenode/ispliability_fnl.pdf [https://perma.cc/57ZL-HCN7] (criticizing DMCA take-down procedure).
73. See 47 U.S.C. § 230(c) (noting limited applicability of section § 230); see also Klayman v. Zuckerberg, 753 F.3d 1354, 1359 (D.C. Cir. 2014) (clarifying meaning of “publisher” under statute); Chi. Lawyers’ Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670-71 (7th Cir. 2008) (discerning applicability of § 230(c)(1)). While the meaning of “publisher” is not specifically defined in the Act, “publishing” is generally understood as “making the decision [on] whether to print or retract a given piece of content” and a “publisher” is someone who reproduces work for the public. See Klayman, 753 F.3d at 1359.
74. See 47 U.S.C. § 230(f)(2)-(3); infra notes 75-76.
refers to “any information service, system or access software provider that [merely] provides or enables computer access by multiple users to a computer server.” On the other hand, an information content provider is “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.” The determinative factor distinguishing interactive computer service providers from information content providers is responsibility for the creation or development of content. Immunity under § 230 extends only to interactive computer service providers and not to information content providers.

To decide whether immunity under § 230(c)(1) should extend to a particular entity, courts often utilize a three-pronged test, asking: whether an interactive computer service is used or provided; whether the entity can be considered an information content provider of the objectionable content or activity in question; and whether the cause of action seeks to hold the online entity as a publisher or speaker of third-party content. As applied to social media outlets, the first prong is easily satisfied because social media websites clearly

75. See 47 U.S.C. § 230(f)(2); see also Klayman, 753 F.3d at 1357 (concluding Facebook meets definition of interactive computer service). In Klayman, the court determined that Facebook qualified as an interactive computer service because “it is a service that provides information to ‘multiple users’ by giving them ‘computer access to a computer server.’” See Klayman, 753 F.3d at 1357. Compare id. at 1357 (explaining Facebook classification), with Carafano v. Metrosplash, Inc., 207 F. Supp. 2d 1055, 1065-66 (2002) (concluding defendant satisfied requirements of both interactive computer service and information content provider). In Carafano, the court concluded that the ISP in question did not qualify for CDA immunity because it produced the limited set of questions and answers used by its members for their profiles, thereby making it “partly responsible” for the creation of the information. See Carafano, 207 F. Supp. 2d at 1068.

76. 47 U.S.C. § 230(f)(3). For example, in Fair Housing Council, the court held that the service provider was an information content provider because the company was more than a passive conduit of information supplied by others. See Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008). The court concluded the website was an information content provider because users had to create their profiles using a set of questions and answers created by the service. See id.; see also Klayman, 753 F.3d at 1358 (holding provision of neutral tools insufficient to make ISP information content provider). In Klayman, the court held that “provid[ing] a neutral means by which third parties can post information of their own independent choosing online” is insufficient to make a website an information content provider. Klayman, 753 F.3d at 1358.

77. See supra notes 75-76 and accompanying text (discussing factors prompting information content provider liability versus no liability).


79. See Catalano, supra note 78, § 2 (outlining three-pronged test employed by courts construing § 230(c) of CDA). Courts have consistently held that ISPs are considered interactive computer service providers. See id. To determine whether a website is an interactive service provider, courts must first determine whether sufficient evidence indicates that the website “provided or enabled computer access by multiple users to a computer server,” as defined under § 230(f)(2). Id.; see 47 U.S.C. § 230(f)(2).
provide interactive computer services. The main inquiry under the second prong is whether the online entity was, in any way, responsible for the creation or development of information. Occasionally, the court may also consider whether the online entity has “materially contributed” to the third-party’s unlawful conduct. Finally, the third prong of the test requires the court to analyze the plaintiff’s theory of liability, regardless of how it is presented, to decide whether the cause of action ultimately falls within the purview of traditional editorial functions.

4. Judicial Development of Section 230

a. Broad Interpretation of Scope of Immunity

About a year after Congress enacted § 230 of the CDA, in Zeran v. America Online, Inc. the Fourth Circuit Court of Appeals interpreted § 230 as giving broad immunity to ISPs. In Zeran, the plaintiff brought an action against America Online, Inc. (AOL) for failing to promptly remove defamatory messages posted by an anonymous third-party, as well as its refusal to retract those messages and screen for similar postings in the future. At trial, AOL successfully advanced § 230 as an affirmative defense. On appeal, Zeran

80. See supra note 75 and accompanying text (defining and clarifying interactive computer service provider under § 230).
82. See Catalano, supra note 78, § 2 (noting § 230 only applies to information derived from third party). This prong comes from the section of the “statute that requires that the information be provided from ‘another’ information content provider” before immunity from liability is available. Id. Developer liability is not established simply because the plaintiff alleges that the defendant should have known of the possibility that certain tools may facilitate the posting of objectionable content. See Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1197-98 (2009) (explaining provision of neutral tools will not undermine immunity under CDA). A much greater level of involvement is needed from the defendant website. See id.
83. See Catalano, supra note 78, § 2 (laying out third prong of test employed by courts). Traditional editorial functions include decisions on whether to “publish, withdraw, postpone, or alter content”; and only causes of action that seek to hold a service provider liable as the publisher of the content are protected by § 230. See id. (explaining scope of protection under CDA); see also Benjamin Wittes & Zoe Bedell, Did Congress Immunize Twitter Against Lawsuits for Supporting ISIS?, LAWFARE (Jan. 22, 2016), https://www.lawfareblog.com/did-congress-immunize-twitter-against-lawsuits-supporting-isis [https://perma.cc/8C7U-UUR5] (examining whether Congress intended to immunize Twitter for facilitating terrorism).
84. 129 F.3d 327 (4th Cir. 1997).
85. See id. at 329-30 (outlining cause of action); see also REIDENBERG ET AL., supra note 12, at 10 (providing facts of case); Paul Ehrlich, Article, Communications Decency Act § 230, 17 BERKELEY TECH. L.J. 401, 406 (2002) (examining court’s interpretation of immunity under § 230 in Zeran).
86. See Zeran, 129 F.3d at 328-30 (asserting § 230 affirmative defense). In Zeran, an unidentified user of AOL’s bulletin board posted a message advertising the sale of “Naughty Oklahoma T-shirts” containing offensive slogans related to the 1995 Oklahoma City Federal Building bombing. Id. at 329. The plaintiff, Zeran, received several disturbing and harassing phone calls because an unidentified user gave Zeran’s home phone number as the contact for interested buyers. Id. Zeran initiated the lawsuit against AOL when it refused to remove and retract the defamatory postings. Id.
87. See id. at 330 (recounting Zeran’s notice-based liability argument argument).
argued that § 230 only eliminated publisher liability, but not distributor or notice-based liability for third-party content. As such, he argued that AOL should not receive immunity under § 230(c)(1) because it was a distributor, and § 230(c)(1) only protects ISPs from being liable as a “publisher or speaker” of third-party content. The Fourth Circuit rejected Zeran’s argument, reasoning that because the distributor standard of liability is essentially a subset of publisher liability, it is also protected under § 230. In support of its reasoning, the court explained that imposing notice-based liability on computer service providers would frustrate Congress’s two main goals in enacting § 230. Notice-based liability would make computer service providers overly cautious by increasing their incentives to restrict speech, and by discouraging them from self-regulating for fear of being exposed to liability. Practically speaking, given the voluminous number of postings on the Internet, forcing computer service providers to screen every suspicious posting would place an impossible burden on them. Therefore, the court rejected Zeran’s argument to narrowly construe § 230, and instead emphasized that Congress’s desire to “promote unfettered speech on the Internet” necessitates a broader reading of § 230 that protects ISPs from any cause of action originating from third-party content. Because Zeran was the first major case to interpret § 230, the Fourth Circuit’s decision to eliminate notice-based liability and grant broad immunity to ISPs had far-reaching consequences: it set the tone for the judicial development and construction of § 230.

88. See id. at 331 (describing Zeran’s contention AOL fell outside protective scope of § 230).
89. See id. at 331-32 (conveying Zeran’s claim distributor liability distinct from publisher liability).
91. See id. (expressing concern notice-based liability would cause over censorship and deter any regulation of offensive material).
92. See id. (emphasizing heavy burden placed on ISPs by imposing notice-based liability).
93. See id. (rejecting narrow construction of § 230). The court reasoned that notice-based liability would likely have chilling effects on free Internet speech. See id. It would be much easier and more convenient for the service provider to simply remove objectionable postings upon notification as opposed to taking on the burden of screening through endless online content. See id. Notice-based liability would also deter service providers from regulating content posted on their website because such regulation, regardless of whether it was made in good faith, would expose them to potential liability. See id. Lastly, notice-based liability is an easy way for third-party users to sue and blame service providers for any postings with which they disagree. See id. Once the user finds a posting that he or she disagrees with, all that the offended party needs do is “notify” the service provider, alleging that the content is defamatory, and the service provider would be obligated to investigate the allegedly defamatory material. See id. This puts service providers in the impossible position of deciding between suppressing speech and risking liability. See id. Because such perverse outcomes directly contradict the statutory purpose of § 230, the court held that it was unlikely Congress intended to leave notice-based liability intact. Id.
94. See Zeran, 129 F.3d at 333-34 (rejecting narrow reading of § 230).
95. See id. at 334 (setting forth broad construction of § 230); see also REIDENBERG ET AL., supra note 12, at 11 (explaining Zeran court decided furthering congressional objectives requires broad interpretation of § 230).
Following Zeran, the district court in Blumenthal v. Drudge\textsuperscript{96} examined the point at which an ISP becomes an “information content provider.”\textsuperscript{97} The plaintiff alleged that the defendant, Matt Drudge, published a defamatory piece on him while under a licensing agreement with AOL.\textsuperscript{98} Although the licensing agreement placed Drudge in a publisher role and charged him with the responsibility of “creat[ing], edit[ing], updat[ing], and ‘otherwise manag[ing]’ the content,” AOL reserved the right to “remove content that [it] reasonably determin[e]d [was in] violat[ion] [of] AOL’s then standard terms of service.”\textsuperscript{99} The plaintiff sought to impose liability on AOL based on the terms of the licensing agreement that granted AOL specific editorial rights.\textsuperscript{100} Nevertheless, the Blumenthal court declined to impose liability on AOL because Drudge authored the allegedly defamatory piece himself without any substantive contribution from AOL.\textsuperscript{101} The court’s decision in Blumenthal was particularly significant because it found that an ISP does not achieve content provider status simply because it retains some removal or editorial rights in a licensing agreement.\textsuperscript{102}

In Batzel v. Smith,\textsuperscript{103} the Ninth Circuit further clarified the meaning of “information content provider” under § 230, and addressed whether § 230 immunity should extend to an ISP in situations where the posted information was not intended for dissemination.\textsuperscript{104} The defendant in Batzel sent an email to the Museum Security Network (Network) alleging that the plaintiff owned stolen artwork.\textsuperscript{105} After receiving the email, the moderator of the Network’s website and listserv slightly edited the email, posted it on the Network’s website, and sent it to the listserv.\textsuperscript{106} Sometime after the moderator posted the

\begin{footnotesize}
\begin{enumerate}
\item 97. See id. at 49-50 (distinguishing between ISP and information content provider).
\item 98. Id. at 46 (stating plaintiff’s cause of action against defendant). Drudge created a gossip column called the Drudge Report, which featured gossip from Hollywood and Washington D.C. Id. at 47. After entering into this licensing agreement, Drudge published a piece of gossip in his column alleging that the plaintiff, Sidney Blumenthal, the President’s assistant at that time, had a history of spousal abuse. Id. at 46-48.
\item 99. See id. at 47 (setting forth relevant parts of licensing agreement). According to the licensing agreement, Drudge would receive monthly royalty payments of $3,000 from AOL in exchange for making the Drudge Report available to all AOL users for one year. Id.
\item 100. See Blumenthal, 992 F. Supp. at 51 (asserting plaintiff’s contention AOL liable due to editorial control over Drudge).
\item 101. See id. at 50 (reasoning AOL not information content provider and thus, not liable).
\item 102. See Blumenthal v. Drudge, 992 F. Supp. 44, 52-53 (D.D.C. 1998) (concluding AOL immune from liability). Similar to the Zeran court, the Blumenthal court focused its decision on the congressional intent behind § 230: “to encourage the good faith self-regulation of offensive content without fear of liability, even in situations where policing attempts were unsuccessful.” See id. at 52; Zeran v. Am. Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997) (interpreting congressional intent behind enactment of § 230).
\item 103. 333 F.3d 1018 (9th Cir. 2003).
\item 104. See id. at 1032-33 (considering whether unintentional posting by another falls within definition of information content provider).
\item 105. See id. at 1021, 1030-33 (detailing email sent and highlighting differences in statutory definitions of information content provider and ISP).
\item 106. See id. at 1021-22 (providing general background of case).
\end{enumerate}
\end{footnotesize}
revised email, he discovered that the original author of the email neither desired nor intended for the email to be made public. Batzel is yet another example of a court making Congress’s desire to protect free Internet speech the focus of its analysis. In its reasoning, the Batzel court rejected the plaintiff’s claim that making minor edits and deciding what portions of the email to publish made one a “developer” of content under § 230. Instead, the court held that to rise to the level of “creation or development of information,” there has to be “substantial[ly] [more] than merely editing portions of an e-mail and selecting material for publication.”

b. Narrowing the Scope of Immunity: An Emerging Trend?

The Ninth Circuit’s decision in Fair Housing Council v. Roommates.com, LLC is noteworthy because it is one of the few instances where a court narrowed its interpretation of § 230 and held that immunity should not extend to the ISP in question. The court explained that the defendant, Roommates.com, fell outside the scope of § 230 immunity because it created and designed its registration process around questions and answers that it provided to prospective subscribers, which made Roommates.com analogous to an information content provider. The Fair Housing Council decision marked the first major departure from the Zeran decision, and appeared to signify a move toward narrowing § 230 immunity. The Ninth Circuit reasoned that a

107. See Batzel, 333 F.3d at 1022 (suggesting email not intended for publication).
108. See id. at 1027-28 (focusing on Congress’s desire to promote growth of Internet articulated in Zeran). In Zeran, the court concluded that Congress enacted the CDA to promote Internet growth; however, it misunderstood the main objective behind § 230, which was to encourage ISP self-regulation by eliminating liability for unsuccessful attempts at removing defamatory content. See Spiccia, supra note 16, at 403 (addressing Zeran court’s mistake in determining Congress primarily intended to promote Internet growth).
109. See Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003) (rejecting editing and publishing decisions constitute development of information).
110. See id.
111. 521 F.3d 1157 (9th Cir. 2008).
112. See id. at 1167.
113. See id. at 1164-68 (emphasizing service provider’s role in creation of questions and answers). Immunity under § 230 only applies in situations where the ISP is not responsible for “creat[ing] or develop[ing]” the objectionable content. Id. at 1166; see 47 U.S.C. § 230(c)(1) (2012); 47 U.S.C. § 230(f)(3) (establishing scope of protection inapplicable to providers who create content). In Fair Housing Council, the court reasoned that the defendant did more than just provide the means of communication. See Fair Hous. Council, 521 F.3d at 1166 (concluding Roommates.com partially developed content). At the very minimum, the defendant was also responsible for partially developing the information because it forced subscribers to create a user profile prior to utilizing its service; and, more importantly, the profile was based on questions and a limited set of possible answer choices created by the website. See id. The court further reasoned that even though the users were responsible for the creation and development of their own profiles, Roommates.com could still be considered a joint information content provider because it contributed, at least in part, to the development of the information provided. See id.
114. See Fair Hous. Council, 521 F.3d at 1167-68 (clarifying § 230 has limitations); see also REIDENBERG ET AL., supra note 12, at 15 (identifying significance of Fair Housing Council decision); c.f. Fields v. Twitter,
narrower reading was necessary because “development” does not merely refer to editing content, but also to situations where the website “contributes materially to the alleged illegality of the conduct.”\textsuperscript{115} Further suggesting the court’s intention to limit the scope of immunity under § 230, the court opined: “The Communications Decency Act was not meant to create a lawless no-man’s-land on the Internet.”\textsuperscript{116}

House Bill 1865 further indicates a move toward narrowing the scope of immunity under § 230.\textsuperscript{117} When Congresswoman Ann Wagner introduced House Bill 1865 on April 3, 2017, Congress’s asserted purpose was to clarify the existing tension between online sex trafficking laws and § 230.\textsuperscript{118} This conflict reared its head in \textit{Jane Doe No. 1 v. Backpage.com, LLC},\textsuperscript{119} where the First Circuit expressed discomfort with holding that § 230 mandated dismissal of plaintiffs’ sex trafficking claims.\textsuperscript{120} Two conflicting congressional acts resulted in this discrepancy: the CDA, designed to promote the right to freely publish third-party speech, and the TVPRA, intended to protect victims from the tyranny of sex trafficking.\textsuperscript{121}

House Bill 1865 proposes to amend § 230 in several significant ways.\textsuperscript{122} First, the bill suggests amending § 230’s policy statement to state that Congress intends to “ensure vigorous enforcement” against users and providers of ISPs for “sexual exploitation of children or sex trafficking.”\textsuperscript{123} Second, the bill intends to retain an avenue of recovery for victims of sex trafficking by excluding ISPs that violate 18 U.S.C. § 1591 from § 230’s immunity.\textsuperscript{124}

\textsuperscript{115} See \textit{Fair Hous. Council}, 521 F.3d at 1167-68 (suggesting limitations to broad immunity under § 230).
\textsuperscript{116} See \textit{id.} at 1164 (cautioning CDA not without limitations).
\textsuperscript{118} See \textit{H.R. 1865, § 3} (clarifying protection under § 230 not extended to websites facilitating online sex trafficking).
\textsuperscript{119} 817 F.3d 12 (1st Cir. 2016).
\textsuperscript{120} See \textit{id.} at 15, 24 (reacting to tension between Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA) and § 230).
\textsuperscript{121} See \textit{id.} at 15 (elucidating irreconcilability of § 230 and TVPRA due to differing objectives).
\textsuperscript{122} See \textit{H.R. 1865, § 3} (offering suggestions to amend § 230 to facilitate prosecution of online sex traffickers).
\textsuperscript{123} \textit{id.} (amending policy statement).
Lastly, the bill proposes to remove § 230 immunity from those who violate “any State criminal statute that prohibits [the] (i) sexual exploitation of children; (ii) sex trafficking of children; or (iii) sex trafficking by force, threats of force, fraud, or coercion,” and also those who violate “any other Federal or State law that provides causes of action, restitution, or other civil remedies” to such victims.125 Ultimately, while the scope of the proposed amendments appears closely tailored to exclude only ISPs that facilitate online sex trafficking, the proposed bill evidences a clear step toward narrowing the broad immunity that ISPs have enjoyed under § 230.126

5. Criticism of the CDA

The Fourth Circuit’s overly broad construction of § 230 in Zeran laid the foundation for an overexpansion of immunity and resulted in near absolute invulnerability for ISPs.127 In enacting § 230, Congress wanted to incentivize self-regulation among ISPs without the fear of incurring liability. Yet, numerous critics argue that interpreting § 230 as granting broad immunity is contrary to this congressional objective; armed with the knowledge that they are virtually immune from any lawsuit seeking to hold them responsible as a publisher of third-party content, ISPs are less likely to self-regulate.129

More significantly, scholars and academics argue that Zeran’s broad construction of § 230 is unsupported by the statute’s language and legislative history.130 In Zeran, the court completely eliminated distributor liability,

---

125. H.R. 1865, § 3 (listing suggested exclusions under proposed legislation).
128. See DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 170 (2014) (identifying Senate committee’s intent to encourage ISP self-regulation with § 230 safe harbor provision); Spiccia, supra note 16, at 400 (specifying legislative purpose behind enactment of CDA).
129. See Ou, supra note 65, at 459 (arguing broad immunity defeats intended objectives of CDA); see also Ryan J.P. Dyer, Note, The Communications Decency Act Gone Wild: A Case for Renewing the Presumption Against Preemption, 37 Seattle U. L. Rev. 837, 842 (criticizing overexpansion of immunity under CDA); Spiccia, supra note 16, at 401 (stressing broad immunity induces hands-off approach rather than incentivize self-regulation among ISPs).
130. See Spiccia, supra note 16, at 401-02 (contesting broad immunity unsupported by statute or legislative history); see also Ann Bartow, Internet Defamation as Profit Center: The Monetization of Online Harassment, 32 Harv. J.L. & Gender 383, 417-18 (2009) (criticizing overly-broad language in CDA compared to DMCA). Under the DMCA’s current language, ISPs are not given a free pass; rather, their ability to invoke immunity is contingent on their compliance with statutory requirements, evidencing a greater desire to protect copyright owners. See Bartow, supra, at 418. On the other hand, the CDA is written such that the role of the ISP is highly unrestricted, suggesting a lack of desire to protect victims. See id.; see also David Lukmire, Note, Can
reasoning that it is a mere subset of publisher liability, and is thus incorporated into the latter. 131 This led some academics to criticize the Zeran court for overstepping its judicial boundaries; § 230 specifically mentions publisher liability only, and the Zeran court improperly equivocated that Congress’s silence on distributor liability evidenced its intent to eliminate it. 132 Scholars also argue that Zeran misconstrued that Congress’s main objective in enacting § 230 was to promote the growth of the Internet, when in reality, Congress desired to encourage ISP self-regulation. 133 Finally, critics note that Zeran and its progeny, which read § 230(c)(1) as promoting immunity for third-party content only, render subsection (c)(2) meaningless. 134 These critics note that interpreting subsection (c)(1) as providing immunity for ISPs for third-party content defeats the purpose of including subsection (c)(2), which provides an independent avenue of immunity for ISPs that screen third-party material. 135 In fact, in Doe v. GTE Corp., 136 the Seventh Circuit questioned the relationship between subsection (c)(1) and (c)(2), and whether the latter actually establishes “immunity.” 137 Recognizing the statute’s ambiguity, the Seventh Circuit proposed reading “§ 230(c)(1) as a definitional clause rather than as an immunity from liability, [in order to] harmonize the text with the caption.” 138 This proposed reading would only protect an ISP as a “provider or user” when the information came from a third party, but would penalize an ISP as a “publisher or speaker” if it contributed to the content in any way. 139 Conversely, interpreting § 230(c)(1) as providing immunity to ISPs, even when


132. See Spiccia, supra note 16, at 402-03 (suggesting specific reference to publisher liability in statute meant distributor liability remained intact). It is well-established that the common law imposes two different standards of liability—publisher and distributor—and Congress’s choice to focus on publisher liability without mentioning distributor liability was more than a mere coincidence. See id. at 402-03.

133. See id. at 403 (suggesting flaw in Zeran court’s conclusion of broad immunity).

134. See id. at 403-04 (identifying flaw in Zeran reasoning based on rule against surplusage). The rule against surplusage discourages an interpretation of one part of a statute that would render another part of the statute duplicative. See id. at 403 n.134.

135. See id. at 403-04 (questioning relevance of subsection (c)(2) if subsection (c)(1) provides all relevant protection). Interpreting § 230(c)(1) as protecting ISPs from the publication of any third-party content renders § 230(c)(2)—which immunizes ISPs who choose to censor—obsolete. See id.; see also Jonathan A. Friedman & Francis M. Buono, Limiting Tort Liability for Online Third-Party Content Under Section 230 of the Communications Act, 52 Fed. Comm. L.J. 647, 657 (suggesting Zeran decision indicates immunity from all tort claims arising from third-party users).

136. 347 F.3d 655 (7th Cir. 2003).

137. See id. at 659-60 (grappling with various possible readings of statute). Immunity is defined as: “Any exemption from a duty, liability, or service of process.” Immunity, BLACK’S LAW DICTIONARY (10th ed. 2014) (emphasis added).

138. See GTE Corp., 347 F.3d at 660 (questioning likelihood Congress intended to discourage self-regulation among ISPs).

139. Id. (reasoning if § 230(c)(1) read to give ISPs immunity, then statute’s caption conflicts with text).
they refrain from filtering or censoring, conflicts with Congress’s intent to encourage self-regulation amongst ISPs.  

B. Overview of the Civil Remedy Provision of the Antiterrorism Act (ATA)

1. The ATA: Legislative History, Purpose, and Framework

Prior to Congress’s enactment of the ATA, American victims of overseas terrorist acts had no legal recourse unless they were specifically identified as “compensable victims under relief statutes covering the specific terrorist incident.” Family members of direct victims had even weaker statutory claims, even though they arguably suffered as much as actual victims. Consequently, the statutory schemes that existed before the ATA were inadequate to compensate all victims, regardless of whether or not the statute explicitly addressed the victim. Although these victims often petition courts to address their lack of legal recourse by expanding their right to compensatory relief, such plaintiffs face other inherent difficulties.

Through the ATA, Congress provided American victims with access to civil damages for acts of international terrorism. The ATA supplements preexisting extraterritorial criminal jurisdiction by allowing victims to seek civil remedies against the perpetrators of international terrorist acts. Prior to

140. See id. (doubting § 230(c)(1) intended to allow ISPs to take hands-off approach in content regulation); Spiccia, supra note 16, at 404 (asserting broad construction of § 230 improper and against legislative intent); see also Ali Grace Zieglowsky, Note, Immoral Immunity: Using a Totality of the Circumstances Approach to Narrow the Scope of Section 230 of the Communications Decency Act, 61 HASTINGS L.J. 1307, 1313-1314 (2010) (claiming manipulation and expansion of immunity Congress intended to grant under CDA). Instead of trying to apply a bright line rule, courts should take a totality of the circumstances approach, and consider all the facts and circumstances of each individual case. See Zieglowsky, supra, at 1325 (advocating for totality of the circumstances approach despite decrease in predictability); see also Lukmire, supra note 130, at 398 (arguing broad immunity under CDA contradicts goal of encouraging Internet responsibility).
141. See Rosenfeld, supra note 18, at 732 (commenting on lack of legal recourse for terror victims prior to ATA).
142. See id. at 732-33.
143. See id. at 733-34.
144. See id. at 734-35 (highlighting compensation difficulties prior to ATA); see also Harold Hongju Koh, Civil Remedies for Uncivil Wrongs: Combating Terrorism Through Transnational Public Law Litigation, 22 TEX. INT’L L.J. 169, 181-83 (1987) (identifying various obstacles for victims seeking recovery in courts).
145. See 18 U.S.C. § 2333(a) (2012) (providing civil remedy provision of ATA). Section 2333(a) provides:

Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney’s fees.

Id.
the ATA, victims of tortious acts committed abroad were often left with no legal recourse or insufficient remedies.\[147\] The ATA now provides victims with the ability to seize terrorist “assets [that are] within . . . jurisdictional reach.”\[148\]

The ATA establishes a three-pronged definition of international terrorism.\[149\] Section 2331(1) defines “international terrorism” as acts that: are violent, dangerous, or criminal; appear directed at intimidating or coercing civilians or government; and either occur outside the United States, or have international consequences.\[150\] Even though Congress intended for the legislation to protect American nationals, the statutory language could be broadly construed as to also allow indirect victims an avenue of recourse.\[151\]

Essentially, the ATA furnishes federal courts with the extraterritorial jurisdiction needed for victims to seek civil relief where it had previously been unavailable.\[152\] Defendants in criminal proceedings brought under the ATA are estopped from denying the essential allegations in a subsequent civil trial arising from the same nucleus of facts.\[153\] Importantly, the ATA also provides for treble damages and legal costs, including attorney’s fees.\[154\]
Notably, the language under the civil remedy provision of the ATA fails to indicate exactly who can be sued. As previously provided, the definition of terrorism under § 2331(1) focuses mainly on the nature of the terrorist acts, without providing a description of who those terrorist actors may be. Consequently, victims of international terrorism often attempt to base their theories of liability on this provision, as it gives them the ability to hold multiple entities responsible for acts of terrorism.

When Congress first introduced the ATA in 1987, the legislation largely centered on restricting association or dealings with the Palestinian Liberation Organization (PLO), a designated terrorist organization. Congress enacted the second version of the ATA in 1990, which included several new additions such as the civil remedy provision. Klinghoffer v. S.N.C. Achille Lauro Ed Altri-Gestione Motonave Achille Lauro in Amministrazione Straordinaria helped spur the 1990 amendments, which provided a more substantial form of relief for American victims of international terrorism.

2. Accomplishments and Shortcomings of the ATA

The most significant accomplishment achieved by the ATA is that it provides a previously unavailable mechanism through which indirect victims—such as family members—may seek civil redress against terrorists. Furthermore, the ATA provides a direct civil cause of action against terrorists and, as a result, federal courts are no longer concerned with statutory interpretation and foreign policy issues. Nevertheless, the ATA eliminates

155. See Alison Bitterly, Note, Can Banks Be Liable for Aiding and Abetting Terrorism?: A Closer Look into the Split on Secondary Liability Under the Antiterrorism Act, 83 FORDHAM L. REV. 3389, 3396 (2015) (identifying ambiguities in § 2333(a)).
156. See id. (claiming definition of terrorism in § 2331(1) does not describe terrorist actor); see also 18 U.S.C. § 2331(1) (2012) (defining meaning of terrorism subject to Act).
157. See Bitterly, supra note 155, at 3396 (stating terrorism victims capitalize on ambiguity in statutory language to sue various entities).
158. See id. at 3397 (discussing legislative history of ATA).
159. See id. (detailing inclusion of civil remedy provision in second version of ATA).
160. 921 F.2d 21 (2d Cir. 1990).
161. See Rosenfeld, supra note 18, at 735-36 (recognizing motivation behind 1990 enactment of ATA). Klinghoffer arose out of the October 1985 hijacking of the Achille Lauro ship, allegedly perpetrated by members of the PLO. Klinghoffer, 921 F.2d at 22-23. The nature of the incident, and the inherent difficulties the plaintiffs experienced in their attempts to seek justice, motivated Congress to finally enact the legislation necessary to provide compensation for victims of terrorist attacks. See H.R. REP. NO. 102-1040, at 5 (1992). In the report, the committee identified Klinghoffer as instrumental in initiating the movement toward establishing a civil cause of action for American victims of international terrorism. See id.; see also Rosenfeld, supra note 18, at 736 (explaining Congress’s motivation to enact ATA civil remedy provision).
162. See Stratton, supra note 18, at 30 (stressing legal accomplishment of ATA).
163. See Rosenfeld, supra note 18, at 741-42 (articulating improved statutory scheme for victims under ATA). Without comprehensive legislative guidance on the issue of civil recovery for terrorist victims, federal courts became the arbiters of the legal standards surrounding international terrorism, which often led to conflicting decisions. See id. at 729-31, 729 n.12; see also Koh, supra note 144, at 173 (comparing civil and criminal remedies against terrorists and commenting on lack of legislative guidance).
some, but not all, of the obstacles that plaintiffs seeking civil damages from terrorists encounter, some of which are potentially insurmountable. For example, one of the most common problems plaintiffs face is the difficulty of identifying the perpetrator of a specific terrorist attack. Even when the identity is known, however, it is difficult to apprehend these perpetrators and take them to court as opposing parties. Terrorists themselves are also unlikely to have meaningful assets, and even if they do, their assets are unlikely to be within jurisdictional reach. Instead, plaintiffs’ best option may be to target the organizations, businesses, or nations that help fund terrorist organizations as opposing parties; however, these entities are likely unknown or unidentified. In many instances, the biggest obstacle for plaintiffs is the inherent difficulty in enforcing judgments against terrorists because the assets are likely located overseas, and the procedural and jurisdictional hurdles that exist in trying to attach foreign assets often prove impossible to overcome. Therefore, while the ATA provides an avenue of redress for victims, compensation is far from guaranteed.

C. Section 230 Bars Plaintiffs’ Claims Under the ATA

Family members of terror victims recently sued social media conglomerates

164. See Rosenfeld, supra note 18, at 742 (contending ATA solves some, but not all problems for victims seeking redress).
165. See id. (cautioning against remaining difficulties for plaintiffs).
166. See id.
167. See id. at 743 (arguing terrorists’ assets either nonexistent or hard to acquire).
168. See Rosenfeld, supra note 18, at 743 (observing difficulties of trying to bring entities funding terrorists into court). Most notably, it is difficult to obtain personal jurisdiction over these terrorist-funding entities, as plaintiffs must still satisfy the minimum contacts requirement. Id. at 743-44.
169. See id. at 744; see also Koh, supra note 144, at 183, 183 n.56 (providing instances where plaintiffs failed to enforce civil judgments against foreign terrorists).
170. See Rosenfeld, supra note 18, at 744-45. Compare Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, sec. 2, 130 Stat. 852, 852-53 (2016) (expanding on ability of victims to seek civil redress under ATA), with 18 U.S.C. § 2339B (2012) (defining provision of material support to known terrorists). The Justice Against Sponsors of Terrorism Act (JASTA) states that “[p]ersons, entities, or countries that knowingly or recklessly contribute material support or resources, directly or indirectly, to persons or organizations that pose a significant risk of committing acts of terrorism . . . should reasonably anticipate being brought to court in the United States to answer for such activities.” 130 Stat. at 852. The purpose of JASTA is “to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against person, entities, and foreign countries . . . that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities.” Id. at 853. In essence, JASTA expands a plaintiff’s ability to bring a cause of action against terrorists by explicitly allowing them to base their claim on secondary liability. See Bitterly, supra note 155, at 3400. JASTA amends 18 U.S.C. § 2333(a) by providing that “liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism.” 130 Stat. at 854; see Gonzalez Complaint, supra note 2, at 2 (seeking damages from Google for materially supporting terrorists, pursuant to JASTA amendment to ATA).
such as Twitter, Facebook, and Google, seeking monetary damages. The plaintiffs’ underlying allegations are that, through their intentional provision of accounts and services to foreign terrorist organizations, these social media companies provided material support to terrorists in violation of the ATA. While some of these cases are still pending judgment, one of the cases—Fields v. Twitter, Inc.—has already been dismissed twice.

In Fields, the widow of a government contractor killed in Amman, Jordan, sued Twitter pursuant to 18 U.S.C. § 2333(a), alleging Twitter provided material support to ISIS by knowingly permitting ISIS to use their social media services to recruit, fundraise, and spread terrorist propaganda. The court granted Twitter’s original motion to dismiss, stating that, “[a]s horrific as these deaths were, under the CDA, Twitter cannot be treated as publisher or speaker of ISIS’s hateful rhetoric and is not liable under the facts alleged.” Under the CDA, it is irrelevant how plaintiffs choose to frame their causes of action. What matters most is “whether the cause of action inherently

171. See, e.g., Second Amended Complaint at 1, 16, Fields v. Twitter, Inc., 217 F. Supp. 3d 1116 (N.D. Cal.), aff’d, No. 16-17165, 2018 WL 626800 (9th Cir. 2018) [hereinafter Fields Complaint] (seeking compensatory and treble damages, in addition to other equitable relief); Force Complaint, supra note 2, at 60 (demanding minimum of $1 billion in compensatory damages); Gonzalez Complaint, supra note 2, at 109-10 (suing for treble damages, costs and fees, plus other equitable relief).

172. See 18 U.S.C. § 2339A (2012) (prohibiting intentional provision of material support to terrorists); Fields Complaint, supra note 171, at 2, 6 (asserting Twitter proximately caused plaintiff’s injuries by knowingly and recklessly providing accounts to ISIS); Force Complaint, supra note 2, at 2-3 (alleging Facebook provided known terrorist organization with tools to further terrorist operations); Gonzalez Complaint, supra note 2, at 2, 5 (claiming social media websites materially and knowingly supported terrorists through use of services).

173. 217 F. Supp. 3d 1116 (N.D. Cal. 2016), aff’d, No. 16-17165, 2018 WL 626800 (9th Cir. 2018).

174. See Fields, 217 F. Supp. 3d at 1118 (dismissing case against Twitter for second time because claims barred by CDA); Fields v. Twitter, 200 F. Supp. 3d 964, 966 (N.D. Cal.) (dismissing original complaint pursuant to CDA without prejudice and with permission to amend).

175. See Fields Complaint, supra note 171, at 1-2 (summarizing cause of action against Twitter).

176. See Fields, 200 F. Supp. 3d at 966 (declaring plaintiff’s ATA claim against Twitter barred by § 230); c.f. Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) (confirming “[§] 230 immunity applies even after notice . . . of . . . unlawful nature of . . . third-party content”). But see S. REP. NO. 114-295, at 1 (2016) (identifying congressional desire to constrict terrorist use of social media platforms). The Committee on Homeland Security and Governmental Affairs stated that it intended for Senate Bill 2517—the Combat Terrorist Use of Social Media Act of 2016—to help develop ways by which the United States could combat social media use by terrorists and terrorist organizations. See id.; see also Counterterrorism Hearing, supra note 9, at 12 (statement of Andrew Aaron Weisburd, Director, Society for Internet Research) (arguing necessary to limit terrorists’ social media usage and presence). Mr. Weisburd argues that “service provider[s] who knowingly assist[,] in the distribution of terrorist media [should also] be culpable” and ISPs “must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations, nor can they continue to put the onus of identifying and removing terrorist media on private citizens.” Counterterrorism Hearing, supra note 9, at 12.

177. See Barnes v. Yahoo, 570 F.3d 1086, 1101-02 (9th Cir. 2009) (stressing irrelevance of how plaintiff frames cause of action); Catalano, supra note 78, § 2 (emphasizing § 230 immunity turns on whether complaint seeks to hold defendant liable for third-party content).
requires the court to treat the defendant as the ‘publisher or speaker’ of content provided by another.”

In Fields, the plaintiff tried to circumvent this obstacle by arguing that she was not attempting to impose liability on Twitter as the publisher of content; rather, the essence of her claim was that Twitter’s provision of accounts to ISIS enabled the organization to spread extremist propaganda and other abominable content. Nevertheless, the court reasoned that regardless of how the plaintiff chose to frame her cause of action, the underlying claim still sought to impose liability on Twitter as a publisher of third-party content, which is the exact type of action barred by the CDA. The court further explained that the only difference under plaintiff’s “provision of accounts theory” was that plaintiff sought to impose liability on Twitter for its decisions on who may have accounts, as opposed to what may be posted by those accounts. Such a decision, however, is still a content-based, publishing decision protected by § 230 because it is impossible for Twitter to make the ISIS connection “without analyzing some speech, idea or content expressed by the would-be content holder.” The cases following Fields have not yet been definitively decided, but many scholars believe that they will suffer the same fate: dismissal of the complaints due to CDA immunity.

178. See Barnes, 570 F.3d at 1101-02 (highlighting significance of whether complaint seeks to hold defendant liable for third-party content).

179. See Fields Complaint, supra note 171, at 2, 6 (alleging Twitter’s provision of accounts to ISIS expanded its communicative reach).


181. See id. at 1122-27 (rejecting plaintiff’s “provision of accounts theory”).

182. See Fields, 217 F. Supp. 3d at 1123.

III. ANALYSIS

A. Social Media and Modern Terrorism

When Congress enacted § 230 in 1996, it operated under the belief that the Internet was meant to facilitate the free exchange of words and ideas online, and as such, should be minimally regulated.184 Nevertheless, twenty years have passed since Congress enacted § 230, and the Internet has evolved into something entirely different.185 Today, the Internet “facilitates almost instant communications” and users can easily share or distribute potentially limitless information to a large audience, uninhibited by geographical boundaries.186 Social media websites and video streaming tools add to this sharing process by encouraging connections between people with similar interests.187

The Internet is integral to modern terrorism because it is “global and diffusive,” decentralized, inexpensive, innovative, and allows terrorists to remain anonymous and operate clandestinely.188 Terrorist organizations depend on social media to connect them to supporters and sympathetic audiences, so that they can indoctrinate, recruit, spread propaganda, and legitimize violence.189 For example, Omar Mateen, the perpetrator of the one of the deadliest mass shootings in U.S. history, was partly radicalized through the Internet.190

Evidently, the use of social media websites is critical to terrorist operations, and ISPs are indirectly contributing to terrorist causes.191 The impact § 230 has on the civil liability of ISPs with respect to web-based content cannot be underestimated.192 As a result of § 230 and the Zeran court’s broad

184. See 47 U.S.C. § 230(b)(2) (2012) (elucidating minimal government regulation required to preserve vibrancy and competitiveness of online market); see also Bolson I, supra note 1 (acknowledging nature of Internet originally not suited for regulation).
185. See Bolson I, supra note 1 (commenting on evolution of Internet).
187. See infra note 217 and accompanying text (elaborating how social media promotes friendly connections); see also Tsesis, supra note 10, at 608 (listing various types of information available on YouTube).
188. Cohen-Almagor, supra note 10, at 428 (identifying reasons for modern terrorists’ reliance on Internet).
189. See Tsesis, supra note 10, at 608-09, 612 (positing ISPs play an indirect role in recruitment strategies); see also Chotiner, supra note 8 (recognizing intractable threat posed by lone-wolf terrorists and how Internet facilitates lone-wolf terrorism).
190. Pilkington & Roberts, supra note 8 (affirming lone-wolf terrorist, Omar Mateen, indoctrinated and inspired by online extremist information).
191. See Tsesis, supra note 10, at 608, 612 (demonstrating variety of ways terrorists utilize Internet and social media to operate and recruit).
192. See Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (creating broad interpretation of § 230 and near absolute immunity for ISPs); Bolson I, supra note 1 (lamenting impact of § 230 in discouraging ISP regulation of offensive content); Bolson II, supra note 12, at 9-10 (commenting on far-reaching
interpretation of the statute, ISPs are rarely, if ever, held responsible for web-based content. Not surprisingly, overzealously extending this broad immunity to ISPs neither incentivizes nor motivates them to implement measures that could have a negative impact on traffic and revenue. Victims of harmful or offensive content are often left without legal recourse because § 230 imposes a veritable challenge. To reconcile the revolutionary changes of the Internet with § 230, legislative reform is needed. Although the fight for popularity and revenue amongst various social media websites may act as a disincentive to implementing measures that would adversely affect traffic and earnings, legislation mandating all social media websites to satisfy similar legal obligations would "level the playing field" and alleviate such concerns.

B. Modeling the CDA After the DMCA

A popular proposition among scholars is to model the CDA after the DMCA. Under the DMCA, civil immunity for copyright infringement only extends to ISPs who have met certain requirements, the most important of which is the removal of content upon notification of its infringing nature.

consequences of broad immunity under § 230); Lichtman & Posner, supra note 16, at 34 (criticizing lack of incentive for ISPs to regulate offensive content under § 230).


194. See Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (questioning why law intended to protect good-faith monitoring makes ISPs invulnerable to other liability); Monaghan, supra note 7, at 530 (criticizing lack of incentives for social media websites to implement proper safety measures).

195. See Bolson II, supra note 12, at 10 (recognizing victims of harmful online speech often left without recourse because § 230 precludes liability); Bolson I, supra note 1 (declaring § 230 “greatest threat to a person’s reputation and online privacy”); see also Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1120 (N.D. Cal. 2016), aff’d, No. 16-17165, 2018 WL 626800 (9th Cir. 2018) (dismissing plaintiff’s second amended complaint because still barred by § 230).

196. See Bolson II, supra note 12, at 11-12 (recommending legislative reform to fix flaws with antiquated CDA); Bolson I, supra note 1 (arguing CDA should adapt to technological changes); see also Fields, 217 F. Supp. 3d at 1129 (asserting “Congress, not . . . courts, has . . . authority to amend . . . CDA”); Jia, supra note 14 (questioning legal applicability of twenty-year old CDA in today’s Internet age).

197. See Monaghan, supra note 7, at 530-31 (considering how legislative reform could ease ISPs’ concerns about losing traffic or revenue).

198. See Bolson II, supra note 12, at 14-15 (describing potential legislative changes of CDA modeled on DMCA safe harbor provision); Gerdes, supra note 70, at 672-73 (recommending incorporating elements of DMCA into CDA); see also REIDENBERG ET AL., supra note 12, at 42-44 (discussing literature comparing CDA to DMCA).

199. See 17 U.S.C. § 512(c)(1)(C) (2012) (detailing obligations of ISP before able to invoke immunity). The statute provides: “A service provider shall not be liable for monetary relief . . . if . . . upon notification of claimed infringement . . . [it] responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.” Id.
Following the content’s removal, the content-poster must be notified of the alleged infringement to afford them the opportunity to file a counter-notice to contest the removal.200 If a counter-notice is filed, it is the responsibility of the entity who initiated the removal process to file suit in federal court within ten to fourteen days; failure to do so allows the ISP to repost the allegedly infringing content without fear of liability.201 While a similar amendment to the CDA could address some of the problems associated with § 230, the downside is that a scheme such as the DMCA’s safe harbor provision, without modification, would likely have a chilling effect on free Internet speech.202 For instance, an ISP may be compelled to suppress protected speech simply because too many people are complaining, even if the complaints are only motivated by dislike for the speaker or the content.203 A far more effective approach would be to tailor the notice and removal procedure to the objectives of the CDA.204

C. Revising Section 230’s Good Samaritan Provision

The current judicial trend tends to find that § 230 immunizes an ISP as long as someone else provided the information.205 Without contributing to the creation or development of content, mere knowledge of the illicit nature of third-party content is insufficient to make an ISP the publisher or speaker of

---

200. See id. § 512(g)(2)(A) (requiring reasonably prompt steps to notify subscriber regarding removal or disabling of access to material); id. § 512(g)(2)(C) (allowing subscriber to file counter-notice to dispute removal).

201. See id. § 512(g)(2)(C) (permitting reposting of allegedly infringing content if lawsuit not filed); id. § 512(g)(3)(D) (filing of counter-notice requires entity initiating removal to file suit in federal court).

202. See Bolson II, supra note 12, at 15 (addressing “heckler’s veto” problem); Ciolli, supra note 28, at 158-61 (cautioning against chilling effects on free speech). But see Roter, supra note 70, at 1405-06 (suggesting amending CDA to emulate notice and take down obligation under DMCA). While amending the CDA to include a notice and take down procedure modeled after the DMCA could be effective at resolving some of the issues posed by § 230, imposing such a responsibility on ISPs introduces a new set of problems. See Bolson II, supra note 12, at 15. First, such an obligation merely forces online service providers to engage in a game of “whack-a-mole” with the content-poster, as terrorists and their supporters can simply upload a new post as soon as the old one is removed. See Perlroth & Isaac, supra note 7. Second, the decision on whether to take down content is best left to intelligence experts because there may be strategic value in allowing some postings to continue. See Klein & Flinn, supra note 11, at 58. Lastly, where the line between “terrorist incitement” and the right to free speech is unclear, the threat of take-down liability is likely to incentivize overzealous content removal, which could adversely impact free speech. See Elec. Frontier Found., supra note 70, at 3.

203. See Bolson II, supra note 12, at 15.

204. See id. (recommending tailoring DMCA safe harbor provision to CDA to prevent unintended suppression of protected speech); see also infra Section III.C (contending conditional immunity and temporary suspension better option than immediately removing offending posts).

205. See e.g., Klayman v. Zuckerberg, 753 F.3d 1354, 1358 (D.C. Cir. 2014) (holding social media website not publisher or speaker of content if merely provided neutral platform); Doe v. GTE Corp., 347 F.3d 655, 659-60 (7th Cir. 2003) (noting judicial consensus among circuit courts regarding § 230 immunity); Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (concluding § 230 bars claims against ISP for third-party content).
Based on this line of reasoning, § 230(c)(1) absolves an ISP of civil liability even when it “refrain[s] from filtering or censoring the information on their sites.” This conclusion is hardly logical given that the impetus behind the Good Samaritan provision was to encourage self-regulation among ISPs by refusing to penalize ISPs that chose to regulate, but were nonetheless unsuccessful in doing so. As the Seventh Circuit astutely points out, it seems implausible that a law designed to protect ISPs that engaged in good faith monitoring should “end up defeating claims by the victims of tortious or criminal conduct.” Indeed, it is questionable whether social media websites even qualify for immunity under § 230. Social media websites certainly take a more active role in selecting the kinds of information disseminated on their platforms compared to traditional publishers. Thus, in revising the CDA, Congress should clarify that § 230 does not confer blanket immunity to all ISPs.

Congress should revise § 230 to make immunity conditional on the fulfillment of certain obligations—that is, immunity should only extend to ISPs that make good faith efforts to fulfill their obligations. While this legislative proposal builds off the “duty to report” as proposed in Senate Bill 2372, Senate Bill 2372 is narrow in scope and would only require ISPs to passively monitor for terrorist activity. Congress, however, should amend § 230 to require ISPs to actively monitor for terrorist activity, and withhold immunity from ISPs that knowingly host terrorists on their platform.

Due to the abundance of information and technology available to ISPs, the ISPs themselves are best equipped to monitor potential terrorist activities and

206. See Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) (affirming “immunity applies even after notice of . . . unlawful nature of . . . third-party content”).

207. Doe, 347 F.3d at 659-60 (rationalizing interpreting § 230(c)(1) to provide immunity rather than definitional clause conflicts with statutory purpose).


209. See Doe, 347 F.3d at 660 (considering inconsistency between law’s intended purpose and ultimate result).

210. See Tsesis, supra note 10, at 622-23 (recognizing increased involvement social media sites have with information compared to traditional publishers).

211. See Cohen-Almagor, supra note 10, at 435-36 (maintaining social media websites utilize sophisticated technology for strategic advertisements); Tsesis, supra note 10, at 622-23 (suggesting social media companies more than just passive conduits of information).

212. C.f. Doe, 347 F.3d at 659-60 (perceiving possible ambiguity in statute and relationship between § 230(c)(1) and § 230(c)(2)).

213. See id. at 17 (proposing conditioning ISP immunity on performance of certain obligations); Ciolli, supra note 28, at 259-60 (providing discussion of conditional immunity).

214. See Requiring Reporting of Online Terrorist Activity Act, S.2372, 114th Cong. § 2 (2015) (proposing to require ISPs to promptly report actual knowledge of any terrorist activity to authorities); Press Release, Senator Dianne Feinstein, supra note 11 (clarifying ISPs not required to actively monitor or take additional action to uncover terrorist activity).

215. See infra notes 216-232 and accompanying text (articulating recommended revisions to § 230).
postings on their platforms. For example, consistent with the objective of connecting people and friends, social media websites like Facebook are likely to have some sort of mechanism that facilitates the sharing and connecting process. Furthermore, because most social media websites allow users to report offensive photos or videos, social media websites could facilitate their efforts to debilitate terrorist accounts by utilizing some variation of their current reporting systems. For instance, Facebook has a system that allows users to report posts that abuse its terms of use, and explain why they find a photo or video offensive. Social media websites could utilize a similar system that would allow users to report suspected terrorist accounts and provide reasons for why they think the accounts suggest terrorist activity. Because this technology is readily available, entities should be legally required to develop and institute programs that would help ferret out terrorist accounts and activities. ISPs should thus be required to take an active role in monitoring or screening for terrorist content, and to report suspected terrorist activity to experts in federal law enforcement agencies. Under such a statutory revision, immunity would not extend to ISPs that fail to cooperate with law enforcement, or those that fail to institute monitoring programs.  

216. See McLaughlin, supra note 7 (discussing bill requiring social media companies to report suspected terrorist activities); Should Twitter, Facebook Be Liable for a Terrorist Attack?, supra note 7 (questioning whether social media websites should hold liability for terrorist attacks); cf. Jane Doe No. 1 v. Backpage.com, 817 F.3d 12, 16-17 (1st Cir. 2016) (describing use of automated filtering technology to screen out or modify prohibited terms in advertisements); Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1161-62 (9th Cir. 2008) (detailing technology matching subscribers with housing and rooming preferences).  

217. See Monaghan, supra note 7, at 528-29 (recognizing objective of social media websites and elaborating on mechanisms used to encourage friendly connections); Oremus, supra note 9 (detailing use of special algorithm to control what subscribers see on Facebook newsfeed).  

218. See id. at 528-29 (arguing for application of reporting systems already utilized by social media websites in terrorist context).  

219. See id. (describing how Facebook’s reporting system works).  

220. See id. at 528-29 (contending social media companies should monitor and report suspected terrorist activity).  

221. Klein & Flinn, supra note 11, at 57 (contending social media companies should monitor and report terrorist activities).  

222. See Radicalization Hearing, supra note 11, at 7 (statement of Mark D. Wallace, Ambassador, United Nations) (advocating for social media websites to take more proactive role in policing content); Nakashima, supra note 7 (reviewing possibility of new bill obligating social media websites to report terrorist activities). A proposed bill, modeled the Protect Our Children Act of 2008, would require social media sites to engage in such monitoring activities. See Requiring Reporting of Online Terrorist Activity Act, S.2372, 114th Cong. § 2 (2015) (attempting to impose duty to report online terrorist activity on computer service providers); Nakashima, supra note 7; see also 18 U.S.C. § 2258A(a)(1) (2012) (imposing duty to report known child sex trafficking on communication service providers). Under the Protect Our Children Act of 2008, electronic communication service providers and remote computing service providers are legally obligated to report instances of child pornography; any intentional or willful failure to do so results in a substantial fine. See 18 U.S.C. § 2258A(a)(1)-(e)(2) (providing reporting requirements and consequences of failure to report).  

223. C.f. Klein & Flinn, supra note 11, at 56-58 (proposing criminalizing failure to inaugurate compliance programs designed to detect terrorist activity).
This approach would clarify that ISPs can no longer take a hands-off approach to monitoring, nor can they freely claim immunity under § 230.224 Most importantly, § 230 should be revised to categorically withhold immunity from ISPs that have actual knowledge their websites are used to conduct terrorist operations, as well as ISPs that choose to profit off their platforms despite reasonable notice or knowledge that they are hosting content from a terrorist or terrorist organization.225 It is common knowledge that most, if not all, social media websites earn substantial profits from advertising.226 Utilizing specially crafted, sophisticated algorithms, these entities “engage[] in online profiling” to direct users to specific advertisements tailored to their preferences.227 Consequently, social media companies assume a more proactive role than traditional publishers because they make conscious decisions concerning where to direct specific advertisements on their sites.228 Congress intended for § 230 to protect ISPs that merely serve as neutral platforms for the dissemination of information.229 To say that the protections under § 230 also extend to ISPs that profit off strategically selected advertisements seems to inflate § 230 beyond what Congress intended.230 Furthermore, once a social media company has actual knowledge that it is hosting terrorist content on its website, it becomes more than just a neutral conduit.231 Thus, because “§ 230 immunity is [so] deeply entrenched in most

224. See S.2372, § 2 (requiring reporting of online terrorist activities); see also Radicalization Hearing, supra note 11, at 6-7 (statement of Mark D. Wallace, Ambassador, United Nations) (calling for support of social media companies in countering terrorism); Klein & Flinn, supra note 11, at 58 (noting removal decisions regarding suspected terrorist posts best left to experts). But see McLaughlin, supra note 7 (identifying inherent problems with imposing such responsibilities on social media companies).

225. See CIRTN, supra note 128, at 177 (advocating for exclusion of worst ISP actors from § 230 safe harbor provision); see also Brown, supra note 183 (considering possibility of plaintiffs prevailing based on alternative legal theory to circumvent CDA protections). New lawsuits against social media companies allege that the companies should be liable for profiting from selling advertisements to terrorist sympathizers. See Brown, supra note 183 (suggesting § 230 immunity inapplicable because social media websites decide where to place advertisements). But see Jane Doe No. 1 v. Backpage.com, 817 F.3d 12, 17, 24 (1st Cir. 2016). In Jane Doe No. 1, although the defendant ISP profited from advertisements in the “Adult Entertainment” section—where the victims were trafficked from—the court held that § 230’s immunity precluded liability because the cause of action sought to hold the defendant liable as a publisher or speaker of third-party content. See id. (denying relief to victims because § 230 protects against liability for publishing third-party content).

226. See Brown, supra note 183 (considering whether § 230 should immunize ISPs who profit from terrorist-related content).

227. See Cohen-Almagor, supra note 10, at 435-36 (elaborating on how Internet companies use online profiling tools to increase profits).

228. See Tsesis, supra note 10, at 622-23 (suggesting targeted advertisements make ISPs unlike traditional publishers, and not protected by § 230); Brown, supra note 183 (reasoning ISP no longer passive conduit when using algorithms designed to target specific users).

229. See supra notes 75-76 and accompanying text (reiterating ISP protected under § 230 if not an information content provider).

230. See Brown, supra note 183 (stressing § 230 should not apply to ISPs if contributing to content).

231. Tsesis, supra note 10, at 623; see Roter, supra note 70, at 1406 (proposing to withhold § 230 protections from ISPs who knowingly host terrorists).
circuits,” Congress, in revising § 230, must clarify that immunity will not extend to such bad actors.\textsuperscript{232}

\textbf{D. First Amendment Concerns}

Naturally, concerns regarding the potential suppression of free speech are likely to arise if social media websites immediately remove suspected terrorist accounts.\textsuperscript{233} Therefore, instead of immediately removing suspected accounts, online service providers could temporarily suspend them, investigate the allegations, and reinstate the accounts upon conclusion of the investigative efforts.\textsuperscript{234} Such a procedure may result in backlash from various ISPs, which will likely argue that such measures impose punitive and unnecessary obligations upon them.\textsuperscript{235} Nevertheless, there must be boundaries to prevent unrestrained freedom of expression from transgressing into lawlessness, and imposing this investigatory model is a workable compromise between attempting to inhibit online terrorist operations, and preventing the suppression of free speech.\textsuperscript{236}

\textbf{IV. Conclusion}

The Internet has gone through significant changes since Congress enacted § 230 twenty years ago. The power that individual users have in creating and distributing content is largely unrestrained due to a user’s ability to remain

\textsuperscript{232} Tsesis, supra note 10, at 623 (advocating for congressional revision to § 230); see Citron, supra note 128, at 177 (opining § 230 not intended to encompass bad actors).

\textsuperscript{233} See McLaughlin, supra note 7 (raising concerns about suppression of free speech). While the idea of being able to beat terrorists at their own game is appealing, many are skeptical about the practicality of a bill requiring immediate removal of terrorist accounts. See id. For example, there are concerns that the Requiring Reporting of Online Terrorist Activity Act will inevitably expand to other crimes, that overzealous ISPs will overload officials with tips that cannot be properly investigated, and that the bill will adversely impact free speech rights. See id. In response to the free speech concerns in particular, Ambassador Wallace distinguished between merely requiring social media companies to engage in proactive monitoring as opposed to taking down content. See Radicalization Hearing, supra note 11, at 7 (statement of Mark D. Wallace, Ambassador, United Nations). But see McLaughlin, supra note 7 (cautioning ambiguity on meaning of “terrorist activity” may chill Internet speech). According to Ambassador Wallace, getting social media companies to cooperate with efforts to counter online terrorism is essential; it may not necessarily be the ultimate solution to the problem, but at the very least, it demonstrates a united front on America’s intolerance of violent extremists. See Radicalization Hearing, supra note 11, at 6-7.

\textsuperscript{234} See Bolson II, supra note 12, at 17 (calling for modified version of DMCA notice and take-down procedure); see also Nakashima, supra note 7 (repeating First Amendment concerns if social media companies immediately report suspected terrorist activity); cf. 17 U.S.C. § 512(c)(1)(A)(iii) (2012) (withholding copyright infringement liability from ISPs who “remove, or disable access to, [offending] material”).

\textsuperscript{235} See Reidenberg et al., supra note 12, at 6 (noting ISP opposition to increased responsibility and liability); McLaughlin, supra note 7 (contending social media companies not equipped to take on terrorism policing role).

\textsuperscript{236} See Bolson II, supra note 12, at 15 (suggesting court intervention before removal of offensive content to address free speech concerns); Spiccia, supra note 16, at 408 (highlighting potential problems with over-censorship).
anonymous. This anonymity, coupled with the ubiquitous influence of the Internet and social media, allows terrorists to operate on an inexpensive but highly effective platform while remaining elusive.

While the underlying premise of the CDA made sense twenty years ago, the idea that the Internet and ISPs need to be coddled to survive is outdated and untrue. It is time for Congress to reevaluate § 230, and limit the broad immunity ISPs currently enjoy as a result of decisions like Zeran. Emboldened by the all-encompassing protection § 230 seems to offer, ISPs take shelter in their presumed immunity, and remain free to host terrorist content and avoid liability. This hardly seems what Congress intended when it enacted § 230, especially given the physical and economic devastation terror attacks can inflict on a country. “The very essence of civil liberty [is] the right of every individual to claim the protection of the laws”;237 the idea that ISPs require unfettered immunity to thrive is outdated, and Congress’s failure to respond to changing circumstances leaves victims of terrorism with a right, but no remedy.238

Nicole Phe


238. See supra Section II.C (discussing how § 230 bars plaintiffs’ ATA claims). As Chief Justice Marshall aptly reminds us in Marbury: “The government of the United States has been emphatically termed a government of laws, and not of men. It will certainly cease to deserve this high appellation, if the laws furnish no remedy for the violation of a vested legal right.” Marbury, 5 U.S. (1 Cranch) at 163.