Brooklyn Law Review

Volume 83 | Issue 2 Article 16

1-1-2018

Section 230's Liability Shield in the Age of Online Terrorist

Jaime M. Freilich

Section 230's Liability Shield in the Age of Online Terrorist Recruitment

INTRODUCTION

From its outset, the Islamic State of Iraq and Syria (ISIS)[1] has relied on social media to amass followers and gain strength.[2] While it used to be time-consuming and costly to recruit someone to terror, Twitter, Inc. (Twitter) has provided an avenue through which fighters can upload photos in real time of what they are doing to encourage more people to join their cause.[3] Rather than calling on supporters to fight on the front lines, ISIS uses the digital services that have become part of daily life[4] to attract followers who will wage jihad at home.[5] ISIS propaganda is "crafted not just to stir the hearts of potential recruits but also to boost the organization's ghastly brand—to reinforce Westerners' perceptions of the Islamic State and its devotees as ruthless beyond comprehension."[6] ISIS also uses social media to highlight the "lighter side of life in ISIS."[7] One

---

[1] ISIS "is a militant Sunni movement that has conquered territory in western Iraq, eastern Syria, and Libya, from which it has tried to establish the caliphate, claiming exclusive political and theological authority over the world's Muslims." Zachary Laub, *The Islamic State*, COUNCIL ON FOREIGN REL. (last updated Aug. 10, 2016), http://www.cfr.org/iraq/islamic-state/p14811 [https://perma.cc/PPZ2-69HP].

[2] *See* P.W. Singer & Emerson Brooking, *Terror On Twitter How ISIS is Taking War to Social Media—and Social Media is Fighting Back*, POPULAR SCI. (Dec. 11, 2015), http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media [https://perma.cc/9RV5-5AAY]. ISIS "is content to crowdsource its social media activity—and its violence—out to individuals with whom it had no concrete ties . . . [and] it does so openly in the West's most beloved precincts of the Internet . . . ." Brendan I. Koerner, *Why ISIS is winning the social media war*, WIRED (Apr. 2016), https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat [https://perma.cc/Y7D3-GAB9]; Telegraph Reporters, *How Terrorists Are Using Social Media*, TELEGRAPH (Nov. 4, 2014, 4:02 PM), http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html [https://perma.cc/EX5X-BJDM].

[3] *See* Bruce Auster, *Drawn by Twitter and Trained in Syria, Terrorists Could Turn West*, NPR (Feb. 28, 2014), http://www.npr.org/2014/02/28/283999741/drawn-by-twitter-and-trained-in-syria-terrorists-could-turn-west [https://perma.cc/NL6X-MDXP].

[4] Koerner, *supra* note 2.

[5] *See* Singer & Brooking, *supra* note 2; *see also* Koerner, *supra* note 2. Jihad is "a holy war waged on behalf of Islam as a religious duty; *also*: a personal struggle in devotion to Islam especially involving spiritual discipline." *Jihad*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/jihad [https://perma.cc/9ZWN-9B2V].

[6] Koerner, *supra* note 2.

[7] Singer & Brooking, *supra* note 2.

attempt to bolster its online image was ISIS's "Cats of Jihad" campaign where ISIS fighters took pictures of their cats posing with weapons.[8]

Though Twitter has responded to this trend by suspending thousands of accounts with suspected terrorist links,[9] social media companies have generally taken a "laissez-faire approach" to preventing terrorists from using their platforms to promote their illegal agendas, even as their audiences continue to grow.[10] "The sad truth is that extremists have been more agile, aggressive and insidious in their use of social media platforms than governments and the private sector have been in tracking, stopping and preventing them from hijacking the online world."[11] Indeed, ISIS foot soldiers continue to upload amateur videos and images daily.[12] Those videos are then shared throughout the world both by "ordinary users" as well as by "mainstream" news outlets.[13] In fact, a social media monitor found that ISIS created hype about itself and what it stands for by using hashtags that focused on group messaging and by branding "700,000 accounts [that] discuss[ed] the terrorist group."[14]

In recent years, terrorist attackers are often motivated to violent action in part by social media propaganda.[15] In November

---

[8] *Id.*

[9] *See* Nicky Woolf, *Twitter Suspends 235,000 Accounts in Six Months for Promoting Terrorism*, THE GUARDIAN (Aug. 18, 2016, 2:52 PM), https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis [https://perma.cc/GV4E-29FM].

[10] *Why it's so hard to fight extremist propaganda online*, PBS NEWSHOUR (Sept. 7, 2016), http://www.pbs.org/newshour/bb/hard-fight-extremist-propaganda-online [https://perma.cc/P2ZW-ETL5] [hereinafter *Why it's so hard to fight extremist propaganda online*]. Although there is evidence that ISIS is losing territory and, thus, posting less to social media, the economic advantages of recruiting new members online suggests that this issue can and will persist even if ISIS is defeated. *The ISIS Propaganda Slowdown*, ON THE MEDIA (Oct. 14, 2016), http://www.wnyc.org/story/isis-propaganda-slowdown [https://perma.cc/GZU5-RJTF] [hereinafter *The ISIS Propaganda Slowdown*].

[11] *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*, 114 Cong. 7 (2015) (page 2 of linked written statement of The Hon. Mark D. Wallace, CEO, Counter Extremism Project, https://oversight.house.gov/wp-content/uploads/2015/10/10-28-2015-Natl-Security-Subcommittee-Hearing-on-Radicalization-Wallace-CEP-Testimony.pdf [https://perma.cc/QWH5-KZN3]) [hereinafter *Radicalization: Social Media and the Rise of Terrorism*].

[12] Telegraph Reporters, *supra* note 2.

[13] *Id.*

[14] *Id.*

[15] *See* Katie Bo Williams, *Terror experts puzzled by ISIS claim in Las Vegas attack*, HILL (Oct. 2, 2017, 5:24 PM), http://thehill.com/policy/national-security/353518-terror-experts-puzzled-by-isis-claim-in-las-vegas-attack [https://perma.cc/D4VP-6HGF]. Indeed, even when there is no evidence of terrorist connections, the pervasive nature of ISIS social media accounts has allowed ISIS to take credit for terrorist attacks, even if authorities later show that they were not in fact responsible for the violence. Examples of this include ISIS taking credit for an attack on a casino in Manila, and claims that ISIS both planted bombs at Charles de Gaulle Airport in France and inspired Stephen Paddock—the shooter in the tragic Las Vegas attack. *Id.*

2015, Anwar Abu Zaid, a "lone wolf" representative of ISIS shot and killed two government contractors on an American base in Jordan.[16] Abu Zaid had been moved to terror after watching a video ISIS posted in February 2015 of an execution of a Jordanian pilot.[17] Also in November 2015, more than 100 people in Paris were killed in an attack coordinated by ISIS.[18] The attackers in that instance were radicalized in Europe, and one even attempted to travel to Yemen to fight after he became inspired watching extremist preachers on the Internet.[19] In June 2016, Omar Mateen killed forty-nine people at a Florida night club.[20] Prior to the attack, Mateen downloaded videos of ISIS beheadings.[21] Throughout the three hours he spent in the club before police shot and killed him, Mateen searched for social media references to ISIS and pledged his allegiance to ISIS in conversations with the police.[22]

In the wake of each of those attacks, the families of some of the victims sued social media companies like Twitter and Facebook, Inc. (Facebook).[23] The litigants alleged that the social media platforms provided material support to ISIS in violation of a civil provision of the Anti-Terrorism Act (ATA)[24] since the companies profited from advertisements that ran against the terrorist propaganda.[25] Courts have found organizations to be

---

[16] Fields v. Twitter, Inc., 200 F. Supp. 3d 964, 966 (N.D. Cal. 2016).

[17] *Id.*

[18] Adam Nossiter & Rick Gladstone, *Paris Attacks Kill More Than 100, Police Say; Border Controls Tightened*, N.Y. TIMES (Nov. 13, 2015), http://www.nytimes.com/2015/11/14/world/europe/paris-shooting-attacks.html [https://perma.cc/5NKL-BAQX]. One of the gunmen in the concert hall shouted, "What you are doing in Syria, you are going to pay for it now." *Id.*

[19] Missy Ryan, Emily Badger, & William Booth, *9 young men and their paths to terror in Paris*, WASH. POST (Nov. 21, 2015), https://www.washingtonpost.com/world/9-young-men-and-their-paths-to-terror-in-paris/2015/11/21/edc19464-8ee6-11e5-934c-a369c80822c2_story.html [https://perma.cc/R8FS-7SW2].

[20] Gal Tziperman Lotan, *Families of Three Pulse Victims Sue Facebook, Twitter, Google*, L.A. TIMES (Dec. 20, 2016, 2:58 PM), http://www.latimes.com/nation/os-pulse-social-media-lawsuit-20161220-story.html [https://perma.cc/VHN9-CCHN].

[21] *Id.*

[22] *Id.*

[23] *See generally* Complaint, Crosby v. Twitter, Inc., Docket No. 2:16-cv-14406 (E.D. Mich. Dec. 19, 2016), ECF No. 1 [hereinafter Crosby v. Twitter Complaint]; Amended Complaint, Cohen v. Facebook, Inc., Docket No. 16-cv-4453 (E.D.N.Y. Oct. 10, 2016), ECF No. 17; Complaint, Gonzalez v. Twitter, Inc., Docket No. 4:16-cv-03282 (N.D. Cal. June 14, 2016), ECF No. 1 [hereinafter Gonzalez v. Twitter Complaint]; First Amended Complaint, Fields v. Twitter, 200 F. Supp. 2d 964 (16-cv-00213-WHO), 2016 WL 2586763, ECF No. 21 [hereinafter Fields First Amended Complaint].

[24] Anti-Terrorism Act of 1992, Pub. L. No. 102-572, § 1003(a)(4), 106 stat. 4506, 4522 (codified as amended at 18 U.S.C. § 2333(a) (2012)); *see also supra* note 23 and accompanying text.

[25] Cyrus Farivar, *It'll be Very Hard for Terrorism Victim's Family to Win Lawsuit Against Twitter*, ARS TECHNICA (June 17, 2016, 5:00 AM), http://arstechnica.com/tech-policy/2016/06/itll-be-very-hard-for-terrorism-victims-family-to-win-lawsuit-against-twitter [https://perma.cc/V8CW-7F9F]; Chris Castle, *Live From YouTubeistan: Google Still Providing Material*

liable under the ATA based on evidence that the defendants knew that their funds were being used to conduct acts of terrorism—even if the defendants did not intend for their funds to be used in such a way.[26] Though Twitter, Facebook, and Google may not be giving money to terrorist groups, per se, they are giving terrorist groups a platform to spread their violent rhetoric and they are profiting from those groups' presence on their websites.

Despite the purposes of the ATA, the Communications Decency Act (CDA) has served as an impenetrable shield preventing litigants from successfully bringing suit against social media companies. On August 10, 2016, the United States District Court for the Northern District of California dismissed plaintiffs' claims in *Fields v. Twitter*,[27] holding that the CDA's liability shield for publishers barred the claims.[28] Section 230(c)(1) of the CDA provides a safeguard for interactive service providers (ISPs), preventing them from "be[ing] treated as the publisher or speaker of any information provided by another information content provider."[29] Because of Section 230(c)(1), ISPs are immune from liability when a third party posts content on the ISP's platform and the ISP does not edit or modify that content.[30] Thus, victims' families were unable to seek the legal redress that the ATA was enacted to provide.

Although courts have addressed the Section 230(c) liability shield in other contexts,[31] *Fields* appears to be the first case brought under the ATA where a court used the shield to bar a claim against an ISP.[32] It will be more difficult for future plaintiffs to hold social media companies liable for objectionable content because of the *Fields* court's holding.[33] An amendment

---

Support for ISIS, MUSIC TECH POL'Y (Apr. 28, 2015), https://musictechpolicy.com/2015/04/28/live-from-youtubeistan-google-still-providing-material-support-for-isis [https://perma.cc/DR5N-82A9].

[26] *See, e.g.*, Stephen J. DiGregoria, *If We Don't Bring Them To Court, The Terrorists Will Have Won: Reinvigorating the Anti-Terrorist Act and General Jurisdiction in a Post*-Daimler *Era*, 82 BROOK. L. REV. 357, 378 (2016).

[27] Fields v. Twitter, Inc., 200 F. Supp. 3d 964, 966 (N.D. Cal. 2016).

[28] *See* Communications Decency Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56 137–38 (codified as amended at 47 U.S.C. § 230(c)(1)); *Fields*, 200 F. Supp. 2d at 966.

[29] 47 U.S.C. § 230(c)(1); *see* Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003) (quoting 47 U.S.C. § 230(c)(1)) (defining "information content provider").

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

[31] *See, e.g.*, Jane Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016) (violation of anti-sex-trafficking laws); Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016) (negligent failure to warn); Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014) (intentional assault); Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009) (defamation and negligent undertaking); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2008) (fair housing laws).

[32] *See Fields*, 200 F. Supp. 3d at 970; *see also* 18 U.S.C.A. 2333(a) (West 2016).

[33] *Fields*, 200 F. Supp. 3d at 966–70; Farivar, *supra* note 25.

to Section 230(c) precluding the liability shield's use in cases brought pursuant to the ATA would remedy this issue. Such an amendment is proper because nothing in Section 230's text or history suggests that Congress intended to immunize ISPs from liability in cases related to terrorist activity.[34] Further, the legal landscape must be changed to diminish terrorist organizations' abilities to attract and recruit members online in order to fully protect the American public and prevent future attacks.

Part I of this note briefly reviews the CDA's history and discusses how courts have applied Section 230. It recounts how the *Fields* court used the liability shield to arrive at its decision and analyzes how *Fields* will impact future cases. Part II discusses amending Section 230 and concludes that the amendment would survive a First Amendment challenge. Part III identifies policy issues that will continue to persist even if the government is able to limit speech by terrorist organizations through social media. While there are legitimate policy concerns, the potential benefits of the expanded scope of Section 230 far outweigh the potential harm of continuing to shield social media companies from liability under the ATA.

I. SECTION 230'S LIABILITY SHIELD AND IMPLICATIONS FOR SOCIAL MEDIA COMPANIES

Section 230 of the CDA was enacted to ensure that ISPs would be able to develop a free Internet.[35] To accomplish this goal, legislators included a provision shielding ISPs from liability for illegal content users posted on ISP platforms.[36] Courts have interpreted Section 230 broadly, and in doing so, have reduced the likelihood that ISPs will develop technology and mechanisms to reduce or restrict harmful speech online.[37]

---

[34] The intent of the ATA was to allow American victims to sue terrorist organizations for money damages, and syphoning their money has the potential to prevent them from continuing to operate. 137 CONG. REC. S1771-72 daily ed. Feb. 7, 1991) (statement of Sen. Grassley). Given the key role that social media plays for terrorist organizations, creating incentives for ISPs to prevent terrorist organizations from utilizing their services could further hamper terrorist organizations' abilities to continue to operate, or at the very least, remove some of their influence; *see also* 47 U.S.C. § 230(c)(1) (2012).

[35] *See CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history [https://perma.cc/LEA6-9296] [hereinafter *CDA 230*].

[36] *See* 47 U.S.C. § 230(c)(1).

[37] Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) ("But Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others. In some sort of tacit *quid pro quo* arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to

Absent the threat of a costly legal battle, there are few—if any—incentives to invest money in solutions that would create a better online community. Twitter, relying on prior jurisprudence, utilized Section 230 to completely bar plaintiffs' claims that Twitter violated the ATA;[38] Section 230 will likely continue to bar similar claims against social media platforms.[39]

A. Background and History of Section 230

The CDA "attempt[ed] to regulate obscenity and indecency online."[40] Section 230 of the CDA, a portion of the law introduced in 1995 by Representatives Chris Cox (R-CA) and Ron Wyden (D-OR),[41] responded to two similar cases in New York with conflicting results. In *Cubby, Inc. v. Compuserve, Inc.*, the Southern District of New York found that an ISP could not be held responsible for libel without knowledge of the crime occurring.[42] By contrast, in *Stratton Oakmont, Inc. v. Prodigy Servs. Co*, the New York Supreme Court held that since a website that hosted online bulletin boards moderated its message boards and deleted some messages for "offensiveness and bad taste," the website had become akin to a publisher and should be held responsible for defamatory postings on the website.[43] Even though the cases had differing results, both cases demonstrated the courts' willingness to hold ISPs liable for content posted on their sites if the ISPs were aware of the content's existence. Based on the holdings in *Cubby, Inc.* and *Stratton Oakmont, Inc.*, regardless of how the content came to be, if an ISP was aware of the content, the ISP could be held liable. The two cases concerned Congress because it wanted Internet companies to be "free to develop new and innovative services" and felt that the fear of liability for their users' content would lead ISPs to enact regulations that would ultimately chill online speech.[44]

Therefore, Congress enacted Section 230(c) of the CDA, titled "Protection for 'Good Samaritan' blocking and screening of

---

Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.").

[38] *Fields*, 200 F. Supp. 3d at 966.

[39] Farivar, *supra* note 25.

[40] *CDA 230*, *supra* note 35.

[41] *Id.*

[42] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 141 (S.D.N.Y. 1991).

[43] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 at *4, *7 (N.Y. Sup. Ct. May 24, 1995).

[44] *CDA 230*, *supra* note 35.

offensive material."[45] Section 230 aimed to "encourage the unfettered and unregulated development of free speech on the Internet."[46] It set out to make sure that Internet companies would be immune from liability when acting as publishers of third-party content.[47] Although the Supreme Court struck down the anti-decency portions of the CDA finding that provisions prohibiting transmission or sending of obscene, indecent, or patently offensive communications to persons under eighteen were content-based restrictions on speech that were facially overbroad in violation of the First Amendment,[48] Section 230 and its liability shield survived.

B. Courts' Application of Section 230

Section 230 of the CDA states that, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[49] While Section 230 does not exempt ISPs from all exposure to federal criminal liability,[50] it immunizes ISPs in cases where plaintiffs seek to hold the ISP liable for user-created content.[51]

The enactment of Section 230 prevented certain legal norms from applying to online forums.[52] For example, though a newspaper publisher could be held accountable for content it

---

[45] 47 U.S.C. § 230(c) (2012).

[46] Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) ("The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.").

[47] Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003) ("[T]he telephone company is not liable as an aider and abettor for tapes or narcotics sold by phone . . . so a web host cannot be classified as an aider and abettor of criminal activities conducted through access to the Internet."); *CDA 230*, *supra* note 35; *see also* Backpage.com LLC v. Dart, 807 F.3d 229, 233–34 (7th Cir. 2015) ("As our court has explained, interpreting Section 230(c), 'an intermediary . . . normally is indifferent to the content of what it transmits. Even entities that know the information's content do not become liable for the sponsor's deeds. Does a newspaper that carries an advertisement for "escort services" . . . aid and abet the crime of prostitution, if it turns out that some . . . of the advertisers make money from that activity?'" (citation omitted)).

[48] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997).

[49] 47 U.S.C. § 230(c)(1).

[50] *See Backpage.com*, 807 F.3d at 234 ("It's true that the Communications Decency Act does not immunize the credit card companies or Backpage from federal criminal liability . . . .") (citing 47 U.S.C. § 230(e)(1)).

[51] *Zeran*, 129 F.3d at 330 (4th Cir. 1997).

[52] *Id.*

published,[53] an ISP would be protected from liability when acting as publisher thanks to Section 230. In practice, Section 230 created a form of "Internet exceptionalism."[54] Chief Judge J. Harve Wilkinson of the United States Court of Appeals for the Fourth Circuit noted that Congress's decision to reduce the potential tort claims against ISPs underscores Congress's ultimate purpose of promoting free, unfettered speech on the Internet.[55]

Despite the noble purpose of Section 230, the law failed to create an ideal online community since ISPs remain immune from liability even when they make no attempt to self-police for obscenity or other offensive material.[56] Indeed, given Congress's intent, courts questioned Section 230(c)'s title since the law failed to create an incentive for ISPs to act as "Good Samaritan[s]."[57]

Courts have found the scope of ISP immunity to cover both publishing and distributing liabilities.[58] Publisher liability is very broad—a publisher can be held liable for anything included within the published material—by contrast, "[d]istributor liability is much more limited" and distributors cannot automatically be held liable for material they distribute.[59] The provision of immunity under Section 230 is afforded across all manner of ISPs, including to web hosts,[60] email providers,[61] and websites serving pure commercial

---

[53] *See* Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.D.C. 1998) ("Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared by others."); *accord CDA 230*, *supra* note 35.

[54] H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 369 (2008). "Situated within the larger debate over Internet governance, the concept of Internet exceptionalism presumes that cyberspace cannot be confined by physical borders or controlled by traditional sovereign governments, and thus that cyberlibertarian communities will emerge in which norms of relationship, thought and expression are yet to be formed." *Id.* at 376.

[55] *See Zeran*, 129 F.3d at 331 (4th Cir. 1997).

[56] *See Blumenthal*, 992 F. Supp. at 52 ("Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.").

[57] Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (Judge Easterbrook asked why "should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious . . . conduct?").

[58] Holland, *supra* note 54, at 374.

[59] David Ardia, *Primer on Immunity—and Liability—for Third-Party Content Under Section 230 of Communications Decency Act*, BERMAN KLEIN CTR. FOR INTERNET & SOC'Y (Dec. 17, 2007), https://cyber.harvard.edu/node/93965 [https://perma.cc/MKC5-VBQF].

[60] *See, e.g.*, *GTE Corp.*, 347 F.3d at 655; Doe v. Franco Prods, 2000 WL 816779, at *4 (N.D. Ill. June 22, 2000); *see also* Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 412 (S.D.N.Y. 2001) (Section 230 raised as a defense by web-hosting service, but held not dispositive).

[61] *See* Jane Doe One v. Oliver, 755 A.D. 1000, 1003–04 (Conn. Super. Ct. 2000).

functions.[62] By choosing a broad interpretation of the law,[63] courts "tipped the scales decisively towards efficiency," but not towards decency.[64] In essence, Section 230 created a landscape where ISPs can operate virtually undisturbed by the law, and thus, there are few, if any, legal mechanisms to ensure they are operating in a way that benefits the community at large.[65] By providing immunity to ISPs for both publishing and distributing, Congress left no incentive for ISPs to be innovative to create new ways to remove indecent material from their services.[66]

Beyond allowing immunity for publishing and distributing content, courts interpreted the term "information content provider"—the class for whom there is no immunity—broadly, allowing ISPs to modify content but still benefit from the protections of Section 230.[67] Specifically, those who make "minor alterations" or "take some affirmative steps to edit the material" provided by another do not become information content providers as long as the material's "basic form and message" remain the same.[68] As a result, ISPs remain immune from suit so long as they do not author or greatly alter the content in question.[69] Indeed, since Twitter, Facebook, and Google allow users' to post on their platforms but do not alter users' content, those platforms appear almost permanently immune from suit. If, however, Twitter were to substantially

---

[62] *See* Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 712–14 (Cal. Ct. App. 2002); Schneider v. Amazon.com, Inc., 31 P.3d 37, 40 (Wash. Ct. App. 2001); Stoner v. eBay Inc., 2000 WL 1705637, at *1 (Cal. Super. Ct. Nov. 1, 2000).

[63] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 334 (4th Cir. 1997).

[64] Paul Ehrlich, *Communications Decency Act 230*, 17 BERKELEY TECH. L.J. 401, 402 (2002).

[65] For example, in 2016, Facebook earned at least $100,000 in revenue by selling ads to a Russian company linked to the Kremlin that posted ads to interfere with the 2016 election. An additional $50,000 in ad revenue is suspected to have been purchased by Russian companies, but the 2,200 ads bought "had less certain indications of a Russian connection." Scott Shane & Vindue Goel, *Fake Russian Facebook Accounts Bought $100,000 in Political Ads*, N.Y. TIMES (Sept. 6, 2017), https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html [https://perma.cc/J8HY-PF7J]. In a regime where Facebook cannot be held liable for the content of these ads, Facebook had no reason to question whether it should sell ads to this company. Further, Facebook failed to even realize how these ads were being utilized or the effects they were having on the population at large. Perhaps with a more robust liability regime, Facebook would have taken more responsibility over the content being spread over its platform—content Facebook was profiting from.

[66] Blumenthal v. Drudge, 992 F. Supp. 44, 51–52 (D.D.C. 1998) ("Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.").

[67] 47 U.S.C. § 230(c)(1) (2012).

[68] *See* Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003); Donato v. Moldow, 865 A.2d 711, 724 (N.J. Super. Ct. App. Div. 2005) (quoting *Batzel*, 333 F.3d at 1031).

[69] Ehrlich, *supra* note 64, at 402.

alter a user's Tweet, the liability shield would no longer apply since the suit would be about content *authored* by the ISP.[70]

Although Section 230 grants broad immunity, the statute does not "create a lawless no-man's-land on the Internet"[71] and there have been successful cases against ISPs using other theories of liability. In *Doe v. Internet Brands, Inc.*, the plaintiff sued a website operator for negligent failure to warn, alleging that the defendant knowingly failed to warn her that two individuals were using Internet Brands's website to identify and lure rape victims.[72] Although the plaintiff had posted on the website, the two individuals had not, the court held that plaintiff's claim could move forward since she was not seeking to hold the defendant liable as a publisher of content.[73]

In *Barnes v. Yahoo!, Inc.*, the plaintiff sued Yahoo! claiming that she had relied on its promise to remove explicit photographs her ex-boyfriend had posted online without her consent.[74] The United States Court of Appeals for the Ninth Circuit held that Section 230 did not preclude the plaintiff's promissory estoppel claim because the plaintiff did not "seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached."[75] Since the plaintiff's theory of liability was based on Yahoo!'s "manifest intention to be legally obligated to do something" rather than on its "publishing conduct," Section 230(c) did not bar the claim.[76] The *Barnes* court noted that based on nearly two decades of jurisprudence interpreting Section 230, it is clear that "what matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress—[but] . . . whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content provided by another."[77]

In cases arising under the ATA, however, the analysis should be different. The ATA allows plaintiffs to reach entities a

---

[70] *Cf. id.* (discussing immunity for ISPs so long as they are not content authors); *see also* 47 U.S.C. § 230(c)(1).

[71] Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1162, 1164 (9th Cir. 2008).

[72] Doe v. Internet Brands, Inc., 824 F.3d 846, 849–50 (9th Cir. 2016).

[73] *Id.* The Ninth Circuit emphasized that the plaintiff's negligent failure to warn claim would not require the defendant "to remove any user content or otherwise affect how it publishes or monitors such content. . . . Posting or emailing such a warning could be deemed an act of publishing information, but Section 230(c)(1) bars only liability that treats a website as a publisher or speaker of content provided by somebody else." *Id.* at 851.

[74] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098–99 (9th Cir. 2009).

[75] *Id.* at 1107.

[76] *Id.*

[77] *Id.* at 1101–02.

step removed from the terrorist organizations so long as the entity has "knowledge of and intent to further" the terrorist's violent criminal acts when providing support.[78] The intent of the ATA is to allow American victims of terror the opportunity to sue persons giving material support to terrorists for money damages,[79] and the ATA applies to both legal persons and natural persons alike.[80] Moreover, the Supreme Court has held that the provisions within the ATA prohibiting material support to terrorist groups do not violate the First Amendment right to freedom of speech.[81]

Allowing Section 230 to serve as a complete roadblock to claims arising under the ATA frustrates the ATA's purpose. Further, Section 230's liability shield removes incentives for ISPs to develop mechanisms that will prevent terrorist content from being disseminated through their services.

C. Fields v. Twitter *Expands Section 230's Application*

Section 230 of the Communications Decency Act served as a complete roadblock for the litigants in *Fields*. Absent an amendment altering the scope of the law, future litigants will struggle to successfully bring claims under a civil provision of the ATA.[82]

In November 2015, two U.S. government contractors were shot and killed while working "at a law enforcement training center in Amman, Jordan."[83] The shooter was a Jordanian police officer named Abu Zaid, and in subsequent statements ISIS claimed responsibility for the attack, stating, "Do not provoke the Muslims more than this, especially recruited and supported of the Islamic State. The more your aggression against the Muslims, the more our determination and revenge . . . . [T]ime will turn thousands of supporters of the caliphate on Twitter and others to wolves."[84]

---

[78] John D. Shipman, *Taking Terrorism to Court: A Legal Examination of the New Front in the War on Terrorism*, 86 N.C. L. REV. 526, 539 (2008) (quoting Boim v. Quranic Literacy Inst. & Holy Land Found., 291 F.3d 1000, 1011 (7th Cir. 2002); *see also* 18 U.S.C.A. § 2333(d)(1) (West 2016).

[79] 138 CONG. REC. 33628–29 (daily ed. Oct. 7, 1992) (statements of Sen. Grassley) ("[The ATA] will allow the victims [of terrorism] to pursue renegade terrorist organizations and their leaders, and go after the resource that keeps them in business—their money.").

[80] DiGregoria, *supra* note 26, at 376; 18 U.S.C.A. § 2333(d)(1); *accord* 1 U.S.C. § 1 (2012) (defining "person" to "include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals").

[81] *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 39 (2010).

[82] *See generally* Fields v. Twitter, Inc., 200 F. Supp. 3d 964 (N.D. Cal. 2016) (finding that Section 230 of the CDA precluded plaintiffs from bringing claims against Twitter).

[83] *Id.* at 966.

[84] *Id.* at 967 (alteration in original) (internal quotations omitted).

Instead of alleging that ISIS recruited Abu Zaid through Twitter, the plaintiffs sought to hold Twitter liable on the basis of Twitter violating the ATA[85] by knowingly providing material support to ISIS.[86] Plaintiffs asserted that Twitter's material support included allowing "ISIS to use its social network as a tool for spreading extremist propaganda, raising funds and attracting new recruits."[87] ISIS was able to spread its propaganda and incite fear, according to plaintiffs, by using Twitter to disseminate its official media publications, including publicizing graphic photos and videos of its terrorist feats, thereby spreading propaganda and inciting fear.[88] Plaintiff's also alleged that ISPs used Twitter to interact with potential recruits.[89] Beyond Abu Zaid's one act of terrorism, plaintiffs further alleged that Twitter's "material support has been

---

[85] 18 U.S.C. § 2333(a) ("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.").

[86] *Fields*, 200 F. Supp. 3d at 965. Sections 2339A and 2339B prohibit the knowing provision of "material support or resources" for terrorist activities or foreign terrorist organizations. 18 U.S.C. §§ 2339A(a), 2339B(a)(1) (2012). "[M]aterial support or resources means any property, tangible or intangible, or service," including "communications equipment." *Id.* §§ 2339A(b)(1), 2339B(g)(4). After ISIS captured Maaz al-Kassasbeh, the group launched a Twitter campaign in an attempt to receive ideas for his method of execution. Subsequently, ISIS distributed a twenty-two-minute video of his killing through a Twitter account in February 2015. Although Abu Zaid's brother said he was "moved" by the execution, plaintiffs did not allege that Abu Zaid viewed the video on Twitter or at all, and further "[the] [p]laintiffs [did] not allege that ISIS recruited or communicated with Abu Zaid over Twitter." *Id.* at 966–67.

[87] Fields First Amended Complaint, *supra* note 23, at 1; *see also Fields*, 200 F. Supp. 3d at 965.

[88] *See Fields*, 200 F. Supp. 3d at 965. Indeed, in December 2015, ISIS was circulating "60 individual unique photographs" everyday as part of its propaganda activity to increase morale, recruit supporters, and sustain its momentum in creating the Caliphate. *The ISIS Propaganda Slowdown*, *supra* note 10.

[89] *See Fields*, 200 F. Supp. 3d at 965; *see also* Fields First Amended Complaint, *supra* note 23, at 1. While it used to be time-consuming and costly to recruit someone to terror, Twitter has provided an avenue through which fighters can upload photos of what they are doing in real time in order to encourage people to join their cause. Auster, *supra* note 3. "The reach of the Islamic State's recruiting effort has been multiplied by an enormous cadre of operators on social media. [It] maintains a 24-hour online operation, and its effectiveness is vastly extended by larger rings of sympathetic volunteers and fans who pass on its messages and viewpoint, reeling in potential recruits, analysts say." Rukmini Callimachi, *ISIS and the Lonely Young American*, N.Y. TIMES (June 27, 2015), http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html [https://perma.cc/9DQZ-XHU5]. "Nationwide, more than 80 Americans, mostly young Muslim men, have been arrested for seeking to join the group. Most of those arrested have said they were seduced by ISIS recruiters on social media." Dina Temple-Raston, *ISIS Trial May Offer A Window Into How The Extremist Group Recruits*, NPR (May 10, 2016, 1:02 PM), http://www.npr.org/sections/parallels/2016/05/10/477482627/isis-trial-may-offer-a-window-into-how-the-extremist-group-recruits [https://perma.cc/4975-H5DK].

instrumental to the rise of ISIS and has enabled it to carry out numerous terrorist attacks."[90]

Without reaching an opinion on the merits of plaintiffs' claims, the court dismissed the suit, finding the claims barred by Section 230(c), the "protection for 'Good Samaritan' blocking and screening of offensive material" provision of the CDA.[91] Although plaintiffs contended that their claims were not based on the contents of tweets or Twitter's failure to remove tweets but rather based on the provision of Twitter accounts to ISIS to begin with, the court found such a claim to be problematic.[92] This is because the arguments raised to oppose Twitter's motion to dismiss differed from the allegations in the First Amended Complaint (FAC).[93]

Even if the plaintiffs had alleged that Twitter's liability was based on its provision of accounts to ISIS users in the FAC, their claims still would have been barred. In determining whether Section 230(c)(1) is appropriate in any given case, a court must first determine if the plaintiff is alleging liability based on "the defendant's status or conduct as a 'publisher or speaker.'"[94] If it is, Section 230 applies and it precludes liability for hosting third-party content.[95] The *Fields* court found that provision of accounts falls within the ambit of an ISP's publishing functions since it relates to determining the format and scope of the content to appear online,[96] and Section 230(c)(1) protects ISPs from publisher liability.[97] The court thus dismissed plaintiffs' claims with leave to amend,[98] but in the wake of *Fields* it will certainly be an uphill battle for plaintiffs to successfully

---

[90] Fields First Amended Complaint, *supra* note 23, at 1; *see also Fields*, 200 F. Supp. 3d at 965.

[91] *Fields*, 200 F. Supp. 3d at 968.

[92] *Id.* at 970.

[93] *Id.*

[94] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101–02 (9th Cir. 2009). Nothing in this case indicated that the provision of accounts theory was beyond the scope of Twitter's publishing conduct. *Fields*, 200 F. Supp. 3d at 972.

[95] *Id.*

[96] Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 21 (1st Cir. 2016).

[97] *See, e.g.*, Klayman v. Zuckerberg, 753 F.3d 1354, 1359 (D.C. Cir. 2014) ("[T]he very essence of publishing is making the decision whether to print or retract a given piece of content."); Doe v. MySpace, Inc., 528 F.3d 413, 420 (5th Cir. 2008) ("[D]ecisions relating to the monitoring, screening, and deletion of content . . . [are] actions quintessentially related to a publisher's role."); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1170 (9th Cir. 2008) ("[D]etermin[ing] whether or not to prevent [the] posting" of third-party material online is "precisely the kind of activity" covered by the CDA.); Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003) ("[T]he exclusion of 'publisher' liability necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material").

[98] *Fields*, 200 F. Supp. 3d at 976.

hold social media companies liable for the consequences of terrorists' propaganda dissemination on ISPs' websites.[99]

D. Section 230's Application in the Wake of Fields

Though the *Fields* decision expanded the scope of Section 230(c) to apply even in cases arising under the ATA,[100] the case led to at least one positive development.[101] In its wake, social media companies increased efforts to find and suspend accounts linked with terrorism.[102] Such activity, however, is insufficient. In the event that terrorist material is not removed, plaintiffs seeking to hold companies liable for the material that leads to violent actions[103] will still have to plead their claim in such a way as to avoid Section 230's liability shield,[104] and doing so appears nearly impossible.

An example of one such case is *Gonzalez v. Twitter*.[105] The father of the only American victim among the 130 killed in coordinated attacks at a Parisian soccer stadium, concert venue, and café sued Twitter, Facebook, and Google.[106] He alleged that the three ISPs provided material support to ISIS since they "knowingly permitted the terrorist group ISIS to use their social networks as a tool for spreading extremist propaganda, raising funds and attracting new recruits."[107] Because the complaint's allegations are similar to *Fields*, it appears unlikely that *Gonzalez* will move past the motion to dismiss stage.[108]

---

[99] Farivar, *supra* note 25.

[100] *See supra* Section I.C.; *see also The Twitter Rules*, TWITTER, https://support.twitter.com/articles/18311 [https://perma.cc/A794-G6JC]. Perhaps moving forward, courts will view Twitter rules as a promise made by Twitter that would allow plaintiffs to bring claims under the theory of promissory estoppel, similar to *Barnes v. Yahoo!, Inc.*, 570 F. 3d 1096 (9th Cir. 2009).

[101] Woolf, *supra* note 9; *see also* Jeff John Roberts, *Twitter Shut Down 235,000 Terrorist Accounts This Year*, FORTUNE (Aug. 18, 2016 12:56 PM), http://fortune.com/2016/08/18/twitter-terrorists/ [https://perma.cc/6BZB-EN4Y].

[102] Woolf, *supra* note 9. Between February and August, Twitter reported that it shut down 235,000 accounts and "raised its daily suspension rate by 80% since [2015]." Roberts, *supra* note 101.

[103] Kate Knibbs, *Extreme Moderation: An Organization Says it has a Solution to Curb Terrorist Activity on Social Media. Why Won't Facebook, Twitter, Google, and Other Tech Powers Sign on?*, RINGER (Jan. 17, 2017), https://theringer.com/curbing-terrorist-social-media-activity-facebook-twitter-google-601ff9684068#.z5dy9vb8n [https://perma.cc/8923-MZ2T].

[104] *See* Farivar, *supra* note 25.

[105] *See generally* Gonzalez v. Twitter Complaint, *supra* note 23.

[106] *Id.*

[107] Jacob Bogage, *Family of ISIS Paris attack victim sues Google, Facebook and Twitter*, WASH. POST (June 16, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/16/family-of-isis-paris-attack-victim-sues-google-facebook-and-twitter/ [https://perma.cc/W8NZ-6HDG].

[108] *Cf.* Gonzalez v. Twitter Complaint, *supra* note 23 *with* Fields First Amended Complaint, *supra* note 23; *see also* Farivar, *supra* note 25.

After the Pulse Nightclub attack, the families of three victims brought suit against Twitter, Facebook, and Google in *Crosby et al v. Twitter, Inc. et al.*[109] Plaintiffs alleged that Twitter and other social media companies knowingly provided material support to ISIS[110] since individuals associated with the terrorist group called for donations via Twitter, even going so far as to promote "donation tiers" on the platform.[111] Further, the sites placed advertisements alongside ISIS videos, and thus materially benefitted from hosting terrorist content on their servers.[112] On April 28, 2017, Twitter filed a motion to dismiss, alleging that Section 230 of the CDA barred plaintiffs' claims—notably, *Fields v. Twitter* was the first case cited on Twitter's list of "controlling or most appropriate authorities."[113]

Perhaps the judges hearing the *Gonzalez* and *Crosby* suits will reach different results, but a different interpretation of the law is unlikely because of the consistent determination that Section 230 of the CDA bars claims against ISPs so long as they have not authored or substantially edited the material. It is necessary to amend the law to prevent Section 230's liability shield from precluding judgments in cases brought under the ATA. Plaintiff claims should not be immediately dismissed in cases where courts find that even the inaction of an ISP is the equivalent of providing or attempting to provide material support to a terrorist organization.

II. CONGRESS SHOULD AMEND THE COMMUNICATIONS DECENCY ACT TO PRECLUDE USE OF SECTION 230(C)'S LIABILITY SHIELD IN CASES ARISING UNDER THE ATA

Even though Section 230 was enacted to "encourage online platforms to be proactive about filtering, blocking and sanitizing content," the liability shield has removed incentives to innovate.[114] Because of the shield, the cost of implementing

---

[109] Crosby v. Twitter Complaint, *supra* note 23; Lotan, *supra* note 20.

[110] Crosby v. Twitter Complaint, *supra* note 23.

[111] *Id.* at 12. An ISIS-linked account sought donations for weapons and tweeted that "if 50 dinars is [sic] donated, equivalent to 50 sniper rounds, one will receive a 'silver status.' Likewise, if 100 dinars is [sic] donated, which buys eight mortar rounds, the contributor will earn the title of 'gold status' donor." *Id.* "[O]ver 26,000 Saudi Riyals (almost $7,000) were donated" as a result of that tweet. *Id.*

[112] *Id.* at 13.

[113] Defendants' Joint Motion to Dismiss the Amended Complaint Pursuant to Fed. R. Civ. P. 12(b)(6) at ii, 12–22, *Crosby v. Twitter, Inc. et al,* No. 2:16-cv-14406 (E.D. Mich. Dec. 19, 2016), ECF No. 37.

[114] Arthur Chu, *Mr. Obama, Tear Down This Liability Shield*, TECH CRUNCH (Sept. 29, 2015), https://techcrunch.com/2015/09/29/mr-obama-tear-down-this-liability-shield/ [https://perma.cc/FF5K-L3KT].

tools that could mitigate the impact of online terrorist recruiting outweigh the benefits to social media companies because they remain immune from suit no matter what actions they take or choose not to take.[115]

The current geopolitical climate calls for a renewed look at how courts determine what constitutes incitement.[116] Terrorist communications on online forums should now fall under the incitement standard articulated by the Supreme Court in *Brandenburg v. Ohio* and ISPs should be held liable for allowing such communications to be distributed through their platforms.[117]

A. Congress Should Amend Section 230 of the Communications Decency Act

At the time of its enactment over two decades ago,[118] when the Internet was in its infancy and Mark Zuckerberg was just twelve years old,[119] there was no way for Congress to anticipate that the Internet would be utilized by a terrorist group that did not yet exist.[120] Even if Congress intended for the scope of Section 230 to apply to claims under the ATA, the law was not enacted with the knowledge of how terrorist groups could and would utilize the Internet to recruit members and cause immense harm. Yet this is exactly what has happened.

Just as the CDA does not exempt ISPs from exposure to federal criminal liability,[121] Section 230(c) should not function as

---

[115] *Id.*

[116] Eric Posner, *ISIS Gives Us No Choice but to Consider Limits on Speech*, SLATE (Dec. 15, 2015), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.html [https://perma.cc/6HZ7-TGYX] (noting that the current legal landscape is insufficient to address the threats terrorist pose through their online activities); Cass R. Sunstein, *Islamic State's Challenge to Free Speech*, BLOOMBERG (Nov. 23, 2015, 12:38 PM), https://www.bloomberg.com/view/articles/2015-11-23/islamic-state-s-challenge-to-free-speech [https://perma.cc/WS7J-Z2MW] (same).

[117] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

[118] Communications Decency Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56, 137 (codified as amended at 47 U.S.C. 230 (2012)); *see also* Ehrlich, *supra* note 64, at 402.

[119] *Mark Zuckerberg*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Mark-Zuckerberg [https://perma.cc/2LU6-UYMZ].

[120] Justin Worland, *President Obama Is Not the 'Founder of ISIS.' Here's Who Really Started It*, TIME (Aug. 11, 2016), http://time.com/4448218/donald-trump-isis-founder-president-obama-zarqawi [https://perma.cc/H73L-ZR4N]. In 2013 Abu Musab al Zarqai cut off ties with al-Qaeda and created ISIS to unite the Arab world under a single Sunni regime. *Id.*; *see also* Auster, *supra* note 3; Callimachi, *supra* note 89; Temple-Raston, *supra* note 89.

[121] Backpage.com, LLC v. Dart, 807 F.3d 229, 234 (7th Cir. 2015) ("It's true that the Communications Decency Act does not immunize the credit card companies or Backpage from federal criminal liability . . . ." (citing 47 U.S.C. 230(e)(1) (2012))). Section 230(e)(1), however, only excludes federal criminal prosecutions, not civil lawsuits predicated on federal criminal law. Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL

an immediate bar to claims brought against ISPs when those claims are brought pursuant to the ATA—even when ISPs are mere publishers of third-party content. Because social media companies cannot be sued for damages for content provided by another user, there is no economic incentive to innovate to solve the issue of terrorist propaganda being widely distributed through ISPs.[122] Indeed, even though nonprofit companies are ready and willing to develop systems to identify and block terrorist content,[123] social media companies are not eager to take advantage of such systems.[124] More likely than not, this is because restricting communications of any kind runs contrary to the business models of social media companies. This note proposes adding a subsection to Section 230(c)(1).[125] The amended statute would read as follows:

> (c) Protection for "Good Samaritan" Blocking and Screening of Offensive Material
>
> (1) Treatment of Publisher or Speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (A) This section shall not apply in cases arising under the Anti-Terrorism Act, 18 U.S.C. § 2333.[126]

Allowing claims under the ATA to proceed to trial would create the incentive of avoiding costly litigation and would encourage ISPs to develop creative solutions to reduce the amount of terrorist propaganda online.

B. The Incitement Standard

Since the purpose of Section 230 is to "protect[] vitally important free speech interests,"127 any change to the law would likely result in challenges to the constitutionality of the

---

3813758, at *22 (E.D. Tex. Dec. 27, 2006) ("Section 230 does not limit anyone's ability to bring criminal or civil actions against actual wrongdoers . . . .").

[122] *See supra* note 138 and surrounding text.

[123] Hany Farid partnered with the Counter Extremism Project to create a system to flag terrorist photos. It would automatically remove "the worst of the worst" online content, like beheading videos. Social media, companies, however, "balked" when the Counter Extremism Project proposed this hashing tool to them. Knibbs, *supra* note 103.

[124] *Id.*

[125] 47 U.S.C. § 230(c)(1).

[126] *Id.*

[127] Eric Goldman, *Big Win For Free Speech Online in Backpage Lawsuit*, FORBES (Mar. 17, 2016), https://www.forbes.com/sites/ericgoldman/2016/03/17/big-win-for-free-speech-online-in-backpage-lawsuit [https://perma.cc/K8RZ-CP2X].

alteration. But speech that intends to incite and is likely to incite "imminent lawless action" is not protected by the First Amendment.[128] The proposed amendment to Section 230 would pass constitutional muster because even though the Supreme Court in 1969 could not have anticipated the potential imminent threat that violent discourse could pose through the Internet when it enunciated the current incitement standard in *Brandenburg v. Ohio*, the Court's holding supports the premise that terrorist propaganda is not protected by the First Amendment.[129]

The First Amendment states, "Congress shall make no law . . . abridging the freedom of speech."[130] Accordingly, content-based regulations of speech are viewed as inherently suspect and analyzed under a strict scrutiny standard.[131] Content-neutral regulations of speech aimed at the medium rather than the message are analyzed under an intermediate standard of scrutiny.[132] Although the First Amendment encourages protection of all speech, even speech society finds abhorrent,[133] certain categories of speech are viewed as so contrary to the purposes of the First Amendment that content-based restrictions of speech are permissible.[134] Speech that incites violence is one such category.

Under the most recent iteration of the incitement standard, a state may permissibly regulate speech that advocates violence only if the speech (1) intends to incite and (2) is likely to incite imminent illegal activity.[135] Under the *Brandenburg* test, the government cannot punish speech unless the speech is likely to trigger "imminent lawless action."[136]

A key problem in combatting the issue of terrorist speech with counter-speech is that counter-speech is not likely to

---

[128] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

[129] *See id.*

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

[131] *See* United States v. Playboy Entertainment Group, Inc., 529 U.S. 803, 813 (2000); *see also* CALVIN R. MASSEY, AMERICAN CONSTITUTIONAL LAW: POWERS AND LIBERTIES 823, 826–27 (5th ed. 2016).

[132] Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

[133] United States v. Schwimmer, 279 U.S. 644, 654–55 (1929) (Holmes, J., dissenting).

[134] MASSEY, *supra* note 131, at 829. "The principle categories of unprotected speech are obscenity, child pornography, speech that incites the immediate commission of a crime, and fighting words." *Id.*

[135] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

[136] *Id.* This test ensures strong protection for almost all speech, however, it also creates a situation where "[i]f a person were to say 'The U.S. government should be overthrown' or 'The more acts of terrorism, the better,' or 'All Muslims should join ISIS,' she couldn't be punished unless those statements were likely to produce imminent lawless action." Sunstein, *supra* note 116.

succeed in quelling recruitment efforts.[137] The United States "is seen as lacking credibility by key members of the target audience of people who are vulnerable to IS[IS]'s recruitment tactics."[138] In addition, although the imminence of violent terrorist action may be called into question under the *Brandenburg* formula,[139] there is no question that terrorist speech over the Internet does create a genuine risk of danger.[140] "[S]tudies now posit that mass killings are contagious."[141] Moreover, terrorist groups have become increasingly adept at using social media platforms to "lure young men and women to their mission—without having to risk . . . capture . . . on U.S. soil," thus creating a "radicalization echo chamber" that has "given rise to a[n] historic and unprecedented danger from foreign radicalization and recruitment."[142]

The right to free speech is the cornerstone of a democratic society and governments should consider all options before censoring speech. Despite its importance, this note is not the first instance where the breadth of the free speech right has been challenged. Judge Learned Hand believed that free speech did not protect explicit or direct incitement to violence—even when no harm was imminent—and he rejected the formulaic "clear and present danger" test.[143] Instead he advocated for the test to be applied on a case-by-case basis.[144] Today, legal theorists such as Cass Sunstein

---

[137] *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 114 Congress 92, 98 (2015) [hereinafter *Jihad 2.0*] (statement of Daveed Gartenstein-Ross, Senior Fellow, Foundation for Defense of Democracies).

[138] *Id.*

[139] *See Brandenburg*, 395 U.S. at 447.

[140] For example, during the summer of 2016, a French terrorist suspect killed a police officer and his partner and recorded a Facebook Live video from within his home. Knibbs, *supra* note 103. By the time Facebook shut down his account, "the video had already been ripped and disseminated by sympathizers, journalists, and rubberneckers." *Id.* The Tsarnaev brothers who orchestrated the Boston Marathon bombing "learned how to create pressure cooker bombs from *Inspire*, an online magazine published by the Yemen-based Al Qaeda in the Arabian Peninsula." Azmat Khan, *The Magazine that "Inspired" the Boston Bombers*, FRONTLINE (Apr. 30, 2013), http://www.pbs.org/wgbh/frontline/article/the-magazine-that-inspired-the-boston-bombers/ [https://perma.cc/QD3G-VXZ3]. *Inspire*'s "most meaningful innovation has been to combine both the incitement to jihad with the how-to of terrorism." *Id.* (internal quotations omitted).

[141] Ryan J. Reilly, *Domestic Terrorists Organizing Online Are 'Real Threat,' DOJ Warns*, HUFF. POST (Oct. 14, 2015, 2:10 PM), http://www.huffingtonpost.com/entry/domestic-hate-groups-online-doj_us_561d7491e4b0c5a1ce60f874 [https://perma.cc/PPR5-RUPK]. The Internet allows individuals to organize in ways that previously could only be done through formal meetings. Social media allows people to connect and allows messages to be disseminated by simply clicking send. *Id.*

[142] Posner, *supra* note 116.

[143] United States v. Dennis, 183 F.2d 201, 212 (2d Cir. 1950).

[144] *Id.*

and Eric Posner advocate for a reconsideration of the current incitement standard in light of the current geopolitical climate.[145]

It is appropriate to reexamine the incitement standard by reviewing the Supreme Court's holding in *Dennis v. United States*, since the tense sociopolitical climate when that case arose mirrors that of modern times. In *Dennis* the Court refused to accept the conclusion that the government should not have to wait until plans are about to be put into motion before it is allowed to act.[146] If the government knows that a group "aiming at its overthrow" is working to spread its message and persuade others to join its cause, then the government is permitted—and in fact required—to take action.[147] *Dennis* was decided in 1951 as the Cold War was heating up,[148] and because of that tense sociopolitical climate, the Court held that the distribution of Communist party recruiting materials was sufficiently dangerous to constitute incitement.[149]

The present-day situation is arguably wrought with even more peril. The government is fully aware of ISIS's use of social media for indoctrination and recruitment.[150] Yet the government is barred from acting under the speech-protective incitement standard enunciated in *Brandenburg*.[151] Further, encouraging social media companies to develop better mechanisms to prevent terrorists from using their platforms to disseminate their messages would burden far less speech compared to what the Court allowed in *Dennis*.[152] Importantly, the *Brandenburg* Court would likely support the proposed application of the incitement standard to terrorist propaganda.[153]

Another practical interpretation of the standard would be a combination of Judge Learned Hand's approach with a

---

[145] Posner, *supra* note 116; Sunstein, *supra* note 116.

[146] Dennis v. United States, 341 U.S. 494, 509 (1951).

[147] *Id.*

[148] Geoffrey R. Stone, *ISIS, Fear, and the Freedom of Speech*, HUFF. POST: THE BLOG (Dec. 22, 2015, 3:19 PM), http://www.huffingtonpost.com/geoffrey-r-stone/isis-fear-and-the-freedom_b_8864050.html [https://perma.cc/2378-GP5M].

[149] *Dennis*, 341 U.S. at 509, 516–17.

[150] *See, e.g.*, Scott Shane, Matt Apuzzo, & Eric Schmitt, *Americans Attracted to ISIS Find an 'Echo Chamber' on Social Media*, N.Y. TIMES (Dec. 8, 2015), https://www.nytimes.com/2015/12/09/us/americans-attracted-to-isis-find-an-echo-chamber-on-social-media.html [https://perma.cc/EA82-TTJ9] (A lonely and bored seventeen-year-old in Virginia discovered ISIS online and was gradually drawn into its world. Though he did not start out as a jihadi, he was made into one through the Internet, and was ultimately convicted of the crime of material support of terrorism and sentenced to eleven years in prison after he taught ISIS supports how to transfer funds secretly and drove an ISIS recruit to the airport.).

[151] *See supra* note 135 and accompanying text.

[152] *See supra* note 147 and surrounding next.

[153] *See* Brandenburg v. Ohio, 395 U.S. 444, 447, n.2 (1969) (per curiam).

balancing approach.[154] "If (and only if) people are explicitly inciting violence, perhaps their speech doesn't deserve protection when (and only when) it produces a genuine risk to public safety, whether imminent or not."[155] Under this formulation of the incitement standard, intermediaries could be held liable for allowing the dissemination of videos like ISIS execution videos—these videos are explicit incitements to violence and they are used to inspire others and call people to violence.

Today, it is impossible to know when a danger is imminent, especially in the age of "lone wolf" terrorists.[156] Between 2014 and 2015, there were terror attacks in six countries, all "in the name of radical Islam."[157] In those that took place in Canada and Australia, there is evidence that the attacks were carried out "by a jihadi . . . using social media."[158] It is critical to characterize ISIS-related social media accounts as accounts attempting to incite others to violence, because failing to limit their presence online will allow the threat posed by such terrorist speech to continue to grow without interference.

A greater liability regime would cut off a key lifeline for ISIS and other terrorist organizations.[159] The Internet has become "a dark playground for extremist groups like ISIS" where they "propagandize, radicalize, recruit new members and commit cyber jihad."[160] Moreover, ISIS has become "entirely dependent on the success of its messaging" on the Internet.[161] By

---

[154] Sunstein, *supra* note 116.

[155] *Id.*

[156] Katie Worth, *Lone Wolf Attacks Are Becoming More Common—And More Deadly*, FRONTLINE (July 14, 2016), http://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/ [https://perma.cc/NMN5-BV77] (Lone wolfs are "motivated by a mixture of political and personal grievance" and "dr[a]w some of their radicalization online." In addition, they are difficult to track because they "plot[] the[ir] attack[s] on their own, without direction from or coordination with others.").

[157] *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 11, at 7 (page 4 of linked written statement of The Hon. Mark D. Wallace, CEO, Counter Extremism Project).

[158] *Id.* The attacker used social media either to "spread content pushed out by others, or to leave messages . . . justif[ying] . . . his actions." *Id.*

[159] Some theorists caution us about this approach saying that "countering propaganda is one thing—criminalizing the receipt and distribution of that propaganda is another." David G. Post, *Protecting the First Amendment in the Internet Age*, WASH. POST (Dec. 21, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/21/protecting-the-first-amendment-in-the-internet-age/?utm_term=.083b23dce968 [https://perma.cc/BGP3-FHBV]. It is important to mention that this note's solution does not propose criminalizing the receipt or distribution of propaganda—but rather creating a liability regime wherein ISPs could be held liable for civil damages under the ATA.

[160] *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 11, at 7 (page 2 of linked written statement of The Hon. Mark D. Wallace, CEO, Counter Extremism Project).

[161] *Jihad 2.0*, *supra* note 137, at 90 (statement of Daveed Gartenstein-Ross, Senior Fellow, Foundation for Defense of Democracies). In fact, the pattern in American

revisiting the interpretation of the incitement standard, Congress could constitutionally create an exemption from Section 230 of the CDA to preclude use of the liability shield in cases arising under the ATA. This would increase incentives for ISPs to innovate and develop new solutions to avoid liability by combatting the threat of terror on social media.

III. POLICY CONSIDERATIONS ASSOCIATED WITH AMENDING SECTION 230

Amending Section 230 would create an avenue for legal redress for family members of victims of terrorist attacks while creating incentives for ISPs to develop technology to prevent terrorist propaganda from being posted on their platforms. This new liability regime, however, would not be without its potential externalities since a "hard-and-fast rule against any . . . kind of content . . . shut[s] down the opportunity for discussion around that sort of material."[162]

Some theorists argue that "[u]sing the law to force Facebook and Twitter to do more to block ISIS propaganda would make sense" but such a solution would not solve all problems.[163] They claim that as soon as ISPs "shut down" terrorist communications, it would be easy for jihadis to simply find new websites to spread their message.[164] For example, when Twitter began to shut down more ISIS-related accounts, extremists fled to the Telegram app for more privacy and to prevent themselves from being exiled from all social media platforms.[165] Indeed, the pace at which terrorists find new places to communicate makes it significantly more difficult for ISPs "to keep track of billions of communications."[166] Allowing social media companies to continue with the status quo, however, would be an improper solution because "extremists have been more agile, aggressive and insidious in their use of social media platforms

history "is that in times of national emergency, certain limits on speech will be tolerated." Posner, *supra* note 116.

[162] *Why it's so hard to fight extremist propaganda online*, *supra* note 10.

[163] Posner, *supra* note 116.

[164] *Id.*

[165] Nick Robins-Early, *How Telegram Became the App of Choice for ISIS*, HUFF. POST (May 24, 2017, 5:22 PM), https://www.huffingtonpost.com/entry/isis-telegram-app_us_59259254e4b0ec129d3136d5 [https://perma.cc/XEM7-ZD3Q]; *see also* Elias Groll, *Twitter Suspended Far Fewer Terrorist Accounts in First Half of 2017*, FOREIGN POL'Y (Sept. 19, 2017, 12:46 PM), http://foreignpolicy.com/2017/09/19/twitter-suspended-far-fewer-terrorist-accounts-in-first-half-of-2017/ [https://perma.cc/6PHH-VP8T].

[166] Posner, *supra* note 116.

than governments and the private sector have been in tracking, stopping and preventing them from hijacking the online world."[167]

Others argue that the government should not impose restrictions on what speech can be disseminated over social media.[168] Any social media company could proactively choose to ban pro-ISIS propaganda because the First Amendment does not apply to privately owned websites.[169] Indeed, "YouTube now deputizes some human-rights groups as 'trusted flaggers' to identify ISIS content; Twitter has banned 'indirect threats of violence'; [and] Facebook proactively removes known jihadists from its service."[170] Despite these efforts, the attacks have persisted, and the threat terrorist groups pose through their Internet activity has not lessened. Even as they were losing territory in Iraq, ISIS continued to post "about [twenty] or [twenty-five] unique images" per day.[171] This statistic demonstrates that self-policing is not enough to combat ISIS's online presence.

In addition, Facebook, Twitter, and Google already ban violent threats in their "Terms of Service," but typically do not take down content unless and until forced to do so.[172] "Doing takedowns or removing content goes very much against what they want their platform to do, which is to bring on as much content and discussion as possible because the more content that's there, the more discussion that's there, the more revenue they can generate for their business . . . ."[173] Twitter's dismissiveness of the issue of violent extremists utilizing their platform is exemplified in a quote by a Twitter official who said, "One man's terrorist is another man's freedom fighter . . . ."[174] It even appears that ISPs may be profiting by strategically placing ads alongside ISIS content on their sites.[175] Twitter, Facebook, and Google all target advertisements based on viewers, and their

---

[167] *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 11, at 7 (page 2 of linked written statement of The Hon. Mark D. Wallace, CEO, Counter Extremism Project).

[168] *See* Post, *supra* note 159.

[169] U.S. CONST. amend. I ("*Congress* shall make no law" (emphasis added)); *see also* Laura Sydell, *Pro-ISIS Messages Create Dilemma For Social Media Companies*, NPR: ALL TECH. CONSIDERED (Jan. 29, 2015, 4:54 PM), http://www.npr.org/sections/alltechconsidered/2015/01/29/382435536/pro-isis-messages-create-dilemma-for-social-media-companies [https://perma.cc/XP54-CQ4D] ("[T]he First Amendment does not apply to privately owned websites . . . .").

[170] Singer & Brooking, *supra* note 2.

[171] *The ISIS Propaganda Slowdown*, *supra* note 10.

[172] Sydell, *supra* note 169.

[173] *Id.* (internal quotations omitted).

[174] Jenna McLaughlin, *Twitter Is Not At War With ISIS. Here's Why*, MOTHERJONES (Nov. 18, 2014, 11:30 AM), http://www.motherjones.com/politics/2014/11/twitter-isis-war-ban-speech [https://perma.cc/X4VA-TMAM].

[175] Crosby v. Twitter Complaint, *supra* note 23, at 36.

profits are allegedly "enhanced by charging advertisers extra for targeting advertisements at viewers upon knowledge of the viewer and the content being viewed."[176]

Social media companies are faced with complex criticism because they "are being asked to do more to stop the terrorists," while the government is asking them to "let some of the propaganda to remain" in order to track jihadis.[177] Law enforcement officials want to use the propaganda since they are able to extract information from social media networks in ways that "go beyond traditional investigative techniques."[178] While it may be important for social media companies to keep content up that is useful for law enforcement, they must do so in a way that makes it difficult for alienated and vulnerable youth to find the content.[179]

One way to do so would be through anti-terrorist advertising. Recently, one of Google's subsidiaries, Jigsaw, created a program to place advertising along search results frequently used by ISIS sympathizers to educate them and undo ISIS brainwashing.[180] The program, however, would not be used to track the sympathizers or further identify ISIS sympathizers.[181] It would only be used to educate.[182] In theory, this program could be immensely helpful in fighting ISIS if it is able to successfully strike at ISIS's ability to recruit fighters online.[183] In reality, though, watching videos online once would not be enough—users have to continuously return to the site and, ultimately, users must make a conscious choice to turn away from terrorism.[184] Though the standard remedy for speech that society abhors is counter-speech,[185] it simply does not work effectively in a context such as this one.

Further, even if counter-speech could be effective, families of victims of terrorist attacks should, at the very least, be able to move their lawsuits against social media companies

---

[176] *Id.* at 36–37.

[177] Sydell, *supra* note 169.

[178] *Id.* In addition, the State Department engages in counter tweeting as an important part of the anti-ISIS campaign started by its counterterrorism communications unit wherein State Department tweeters look for ISIS tweets and respond with messages that highlight ISIS atrocities. McLaughlin, *supra* note 174.

[179] Sydell, *supra* note 169.

[180] *See* Andy Greenberg, *Google's Clever Plan to Stop Aspiring ISIS Recruits*, WIRED (Sept. 7, 2016), https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/ [https://perma.cc/QX8S-CR7P].

[181] *Id.*

[182] *Id.*

[183] *See* Singer & Brooking, *supra* note 2; *Why ISIS is Winning the Social Media War*, *supra* note 2.

[184] *See* Greenberg, *supra* note 180.

[185] Stone, *supra* note 148.

beyond the motion to dismiss stage. The proposed amendment is the only avenue through which that would be possible.

CONCLUSION

It is time for Congress to revisit Section 230 of the Communications Decency Act to preclude applicability of the liability shield in cases arising under the Anti-Terrorism Act. Upon challenge, the Supreme Court should uphold the amended law as consistent with First Amendment principles since, in today's geopolitical climate, terrorist recruitment creates a clear and present danger. No longer should companies automatically defeat claims on the grounds that they did not post or edit the material. The families of the victims of terrorist attacks deserve a form of legal redress when the attackers are indoctrinated through social media. ISPs appear to be complicit in the harm since they are not acting as "Good Samaritan[s]"[186] when they fail to take sufficient measures to combat a known threat—ISIS's use of their platform to encourage others to join their terrorist movement.

There is no doubt that Congress and the courts should proceed with caution before altering the legal sphere to place content-based restrictions on speech. Even so, it would be irresponsible to not address this issue as there is a clear tension between individuals seeking to use media platforms to exercise their First Amendment rights and those who utilize those same platforms to incite others to commit violent acts.[187]

"Life, Liberty, and the pursuit of Happiness"[188] is a founding tenet of this country, and it is time this nation places a higher value on "Life" than the economic interests of interactive service providers.

Jaime M. Freilich[†]

---

[186] 47 U.S.C. § 230(c) (2012).

[187] *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 11, at 7 (page 3 of linked written statement of The Hon. Mark D. Wallace, CEO, Counter Extremism Project).

[188] THE DECLARATION OF INDEPENDENCE para. 1 (U.S. 1776).

[†] J.D. Candidate, Brooklyn Law School, 2018; B.S., Cornell University, 2013. Thank you Anne Conroy, Charles Wood, and Alexa Bordner for your tireless efforts, invaluable insights, and enduring patience. Thanks also to Jason George and the entire *Brooklyn Law Review* staff for your help and hard work throughout the year. Special thanks to Ross, whose endless stream of podcasts helped create the foundation of this note. To Eric, Hope, and Stephen, words cannot express my gratitude for your unwavering support and humor. And to my Grandparents, thank you for your endless love and encouragement.