Mark Zuckerberg, Joe Manchin, and ISIS: What Facebook's International Terrorism Lawsuits Can Teach Us About the Future of Section 230 Reform

Kallen Dimitroff[*]

Terrorism thrives on the internet. International terrorist organizations recruit new members, promote extremist ideologies, and operationalize violent attacks through social media platforms. Interactive computer services (ICSs), like YouTube and Twitter, have gone to varying lengths to address international terrorism on their websites. Likewise, many countries have adopted civil mechanisms and regulatory regimes to hold ICSs accountable for their role in international terrorism. The United States has not.

At present, Section 230 of the Communications Decency Act, long considered the "Magna Carta" of the internet, is the centerpiece of America's hands-off approach to content-related internet regulation. Section 230, however, has become one of the most unpopular statutes in Washington—there are currently dozens of bipartisan congressional proposals aimed at repealing or reforming the law. Operationally, Section 230 is an affirmative legal defense that protects ICSs from civil liability arising from user-generated content, including lawsuits involving harm caused by acts of international terrorism. Facebook, the world's largest social media platform, has invoked Section 230 as a legal defense in dozens of lawsuits; it has lost only one.

Using Facebook's Section 230 litigation as its guiding reference, this Note will assess two types of legislative proposals seeking to address ICSs' role in international terrorism: (1) an international terrorism exception to Section 230's protections and (2) a more proactive regulatory regime. Using ISIS and Facebook as case examples, this Note suggests the latter is the superior approach.

---

* Kallen Dimitroff is a J.D. candidate at the University of Texas School of Law. Thank you first and foremost to Professor Jacquelyn Schnieder for teaching a wonderful seminar and encouraging me to submit this Note for publication. Additionally, I am deeply appreciative for hours of conversation with Jay Hulings, Keith Altman, and Kate Gould. Your critical feedback, informed by your respective areas of expertise, was invaluable to the direction of this Note. Thank you also to Professor John Golden and Notes Editors Beth Knuppel, Bryan Hammerschlag, and Mimi Ngyugen for your helpful feedback on various substantive and stylistic points—your contributions undoubtedly strengthened my work. Further thanks to Cooper Shear, Bonnie Devaney, and, my father, Sashe Dimitroff, for providing editorial suggestions that made my writing shine. Finally, thank you to Will McKelvey and Thomas Forster, who patiently listened to me rant about this subject for months. You are all the very best.

Overall, this Note's unique contribution is that its evaluation of Section 230 is grounded in the law's practical consequences. Most evaluations of Section 230 rest on normative assessments or the law's impact on values like free speech and economic growth. But Section 230 is not a moral proposition—it is an affirmative defense to litigation that has expanded beyond its intended scope through decades of judicial interpretation. Thus, this Note seeks to inform the current counterterrorism policy discourse by examining the law in operation. Although a few pieces of legal academic work focus on the difficulties surrounding terrorism and Section 230, none have recommended similar solutions.[1]

1. *See, e.g.*, Ellen Smith Yost, *Social Support for Terrorists: Facebook's "Friend Suggestion" Algorithm, Section 230 Immunity, Material Support for Terrorists, and the First Amendment*, 37 SANTA CLARA HIGH TECH. L.J. 301 (2021) (discussing circuit splits in Section 230 cases, with a particular emphasis on Anti-Terrorism Act litigation); Nicole Phe, Note, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99 (2018) (discussing intermediary liability within the context of Section 230's invocation in Anti-Terrorism Act lawsuits). While both of these pieces discuss constitutional and practical issues presented by Section 230 in the context of international terrorism, neither author considers how her findings may inform the policy discourse surrounding current legislative proposals.

> Illuminating Congress's original intent does, however, underscore the extent of § 230(c)(1)'s subsequent mission creep. Given how far both Facebook's suggestion algorithms and plaintiffs' terrorism claims swim from the shore of congressional purpose, caution is warranted before courts extend the CDA's reach any further.

Force v. Facebook, Inc., 934 F.3d 53, 80 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020) (Katzmann, C.J., dissenting).

Introduction

There are worse places to be a security guard than a gated golf-resort community in Port St. Lucie, Florida.[2] But still, the shifts were long and the rounds were tedious—at least most people would think so.[3] Not Omar.

Omar always wanted a job in law enforcement, so he usually got to work early.[4] However, his behavior was often less than professional: between patrolling PGA Village Verano's rolling golf courses, professional-grade tennis courts, and Spanish-tiled, stucco villas,[5] Omar would blast his fellow guards with racist, sexist, and homophobic remarks.[6] "He was just agitated about everything," a former coworker recalled: "Always shaken. Always agitated. Always mad."[7]

His anger seemingly permeated everything. It spooked his middle school classmates, it ended his first marriage, and it led him to murder forty-

2. *See* Dan Barry, Serge F. Kovaleski, Alan Blinder & Mujib Mashal, *'Always Agitated. Always Mad': Omar Mateen, According to Those Who Knew Him*, N.Y. TIMES (June 18, 2016), https://www.nytimes.com/2016/06/19/us/omar-mateen-gunman-orlando-shooting.html [https://perma.cc/3FQ4-PPZH] (noting Omar Mateen's security guard position was "low-pressure").

3. *See* Anthony Westbury, Nicole Rodriguez & Elliot Jones, *Co-worker: Omar Mateen Homophobic, 'Unhinged,'* FLORIDA TODAY (June 12, 2016, 10:00 AM), https://www.floridatoday.com/story/news/crime/2016/06/12/who-omar-mateen/85791280/ [https://perma.cc/XD7R-JJ88] ("Daniel Gilroy said he worked the 7 a.m. to 3 p.m. shift with G4S Security at the south gate at PGA Village for several months in 2014-15. Mateen took over from him for a 3 to 11 p.m. shift.").

4. Pete Williams, Tracy Connor, Erik Ortiz & Stephanie Gosk, *Gunman Omar Mateen Described as Belligerent, Racist and 'Toxic,'* NBC NEWS (June 13, 2016, 6:36 AM), https://www.nbcnews.com/storyline/orlando-nightclub-massacre/terror-hate-what-motivated-orlando-nightclub-shooter-n590496 [https://perma.cc/HM5Z-HZQY].

5. *See PGA Village Verano Clubhouses and Recreation*, KOLTER HOMES, https://www.kolterhomes.com/new-homes/port-saint-lucie-florida-active-adult-pga-village-verano/lifestyle/ [https://perma.cc/D58X-47FN] (outlining the amenities of PGA Village Verano).

6. Spencer Ackerman, Paul Owens & Ryan Felton, *Pulse Nightclub Shooting: What We Know So Far About the Gunman*, GUARDIAN (June 13, 2016, 3:01 PM), https://www.theguardian.com/us-news/2016/jun/13/omar-mateen-pulse-orlando-shooting-what-we-know [https://perma.cc/L3W2-CRDW].

7. Barry, *supra* note 2.

nine people at Pulse Night Club in Orlando.[8] A few months before the massacre, he became enraged after seeing a pair of men kissing in downtown Miami and concocted a violent plan.[9] A few hours before the massacre, he pledged allegiance to ISIS on Facebook.[10] Like many terrorists, this was not the first time Omar Mateen took to the internet to further his extremist beliefs.[11]

Over the last decade, international terrorist organizations have increasingly used platforms like YouTube and Twitter to recruit new members, plan large-scale attacks, and promote extremist propaganda.[12] Many countries have adopted regulatory regimes that impose burdens on ICSs to curtail terrorists' use of social media.[13] The United States has not.

8. *Id. See also* Gary Detman, *Omar Mateen Had Behavioral Issues in School, Records Show*, CBS 12 (June 16, 2016), https://cbs12.com/news/local/omar-mateen-had-behavioral-issues-in-school-records-show [https://perma.cc/3GXC-GBXK] (reporting that Mateen exhibited behavioral issues in school); Adam Sacasa, *Marriage Certificate Shows Orlando Shooter Married Wife Months After Divorce*, SUN SENTINEL (June 16, 2016, 2:51 PM), https://www.sun-sentinel.com/news/crime/fl-omar-mateen-marriage-certificate-20160616-story.html [https://perma.cc/6WT8-82SA] (reporting that Mateen's first marriage ended in divorce); Ariel Zambelich & Alyson Hurt, *3 Hours in Orlando: Piecing Together an Attack and Its Aftermath*, NPR (June 26, 2016, 5:09 PM), https://www.npr.org/2016/06/16/482322488/orlando-shooting-what-happened-update [https://perma.cc/9EDY-5RUH] (reporting on the events of the Pulse Night Club shooting).

9. Douglas Hanks, *Orlando Shooter's Father Points to Men Kissing in Miami to Explain Son's Anger*, MIAMI HERALD (June 13, 2016, 3:45 PM), https://www.miamiherald.com/news/local/community/miami-dade/article83329252.html [https://perma.cc/NU3B-4LJT].

10. Kevin Sullivan, Ellen Nakashima, Matt Zapotosky & Mark Berman, *Orlando Shooter Posted Messages on Facebook Pledging Allegiance to the Leader of ISIS and Vowing More Attacks*, WASH. POST (June 15, 2016), https://www.washingtonpost.com/world/national-security/investigation-into-orlando-shooting-continues-no-impending-charges-expected/2016/06/15/c3eccf5e-3333-11e6-8758-d58e76e11b12_story.html [https://perma.cc/3DMX-HFME].

11. Alan Blinder, Frances Robles & Richard Pérez-Peña, *Omar Mateen Posted to Facebook Amid Orlando Attack, Lawmaker Says*, N.Y. TIMES (June 16, 2016), https://www.nytimes.com/2016/06/17/us/orlando-shooting.html [https://perma.cc/7KWB-6CPE].

12. *See ISIS Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media: Hearing Before the Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. & Governmental Affs.*, 114th Cong. 1–2 (2016) (statement of Sen. Rob Portman, Chairman, S. Permanent Subcomm. on Investigations) [hereinafter *ISIS Online Hearing*] (explaining that ISIS has mastered modern technology and social media to recruit terrorists and push propaganda). While there has been a rise in acts of domestic terrorism in recent years, such activity is beyond the scope of this Note. *See generally Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 1 (2019) (statement of Hon. Bennie G. Thompson, Member, H. Comm. on Homeland Sec.) ("In the last two years, there have been more domestic terrorism-related arrests than international terrorist-related arrests.").

13. *See, e.g.*, Philip Oltermann, *Tough New German Law Puts Tech Firms and Free Speech in Spotlight*, GUARDIAN (Jan. 5, 2018, 6:36 AM), https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight [https://perma.cc/ZZ7L-YAGY] (outlining Germany's regulatory approach); Heidi Tworek, *International Approaches to Regulating Hate Speech Online: Brief Submitted to the Standing Committee on Justice and Human Rights*, HOUSE OF COMMONS CANADA (May 20, 2019), https://www.ourcommons.ca/Content/Committee/421/JUST/Brief/BR10520161/br-external/TworekHeidi-e.pdf [https://perma.cc/B957-

Section 230 of the Communications Decency Act, often considered the "Magna Carta of cyberspace,"[14] further compounds the problem. The United States not only lacks proactive regulation, but Section 230 also prevents victims of terrorist attacks from using private causes of action to recover against ICSs that provide material assistance to their attackers.[15]

At its core, Section 230 dictates that internet users are liable for the content they create, but ICSs are not.[16] Unfortunately, courts have broadly interpreted Section 230 to preclude liability for almost every kind of civil lawsuit for harm arising from user-generated content, regardless of the harm alleged or ICSs' role in bringing it about. Perhaps this seems facially reasonable. But a close inspection of Section 230 case law reveals the alleged harms range from defamation to murder, and ICSs' alleged roles range from passive failure to remove users' posts to affirmatively employing algorithms that facilitate financial gain.[17] Overall, it seems that no one—except large technology companies and the staunchest free speech advocates—is satisfied with the results.[18]

So, Section 230's days are numbered. In fact, it has become perhaps the most unpopular law in Washington—both former President Trump and President Biden have called for its repeal,[19] and dozens of congressional legislative proposals aim to reform Section 230.[20] Critiques and assessments of various aspects of Section 230 fill hundreds of articles in online publications like *Vox*, *The Verge*, and *Wired*,[21] while Silicon Valley has spent

5ZLD] (outlining Australia's approach and similar proposals in the UK, France, and the European Union).

14. Alan Z. Rozenshtein, *Section 230 and the Supreme Court: Is Too Late Worse Than Never?*, LAWFARE (Oct. 20, 2020, 1:01 PM), https://www.lawfareblog.com/section-230-and-supreme-court-is-too-late-worse-than-never [https://perma.cc/G8DK-JWUL].

15. *See* Fyk v. Facebook, Inc., 808 Fed. App'x 597, 598 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1067 (2021) (holding that Facebook has immunity under § 230(c)(1) because it did not generate the content at issue).

16. *See* 47 U.S.C. § 230(c) (protecting ICSs from civil liability for user-generated content or content moderation).

17. *See infra* Part II (discussing cases in which Section 230 has been used as an affirmative defense).

18. Jonathan Greig, *Section 230 Hangs in the Balance After Attacks from Biden and Trump*, TECHREPUBLIC (Nov. 4, 2020, 7:42 AM), https://www.techrepublic.com/article/section-230-hangs-in-the-balance-after-attacks-from-biden-and-trump/ [https://perma.cc/3NZR-QWPM] (explaining effect of 2020 Presidential election on efforts to repeal Section 230).

19. Rachel Lerman, *Social Media Liability Law Is Likely to Be Reviewed Under Biden*, WASH. POST (Jan. 18, 2021, 8:00 AM), https://www.washingtonpost.com/politics/2021/01/18/biden-section-230/ [https://perma.cc/77GH-ZZ7Q].

20. *See infra* Part IV (discussing the legislative proposals for Section 230 reform).

21. *See, e.g.*, Casey Newton, *Everything You Need to Know About Section 230*, VERGE (Dec. 29, 2020, 4:50 PM), https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation [https://perma.cc/RMX5-X8WB]; Gilad Edelman, *Everything You've Heard About Section 230 Is Wrong*, WIRED (May 6, 2021, 7:00 AM), https://

billions of dollars on lobbying efforts to maintain the status quo.[22] Observers on the left say Section 230 has enabled civil rights violations,[23] and observers on the right say it allows ICSs to censor political speech.[24] This Note, however, suggests that Section 230 has allowed ICSs to avoid accountability for their role in international terrorism.

My thesis is simple: courts are not an effective venue for addressing international terrorists' use of the internet. So, as Congress considers changes to Section 230, it should adopt legislation that allows the Executive Branch to engage in robust regulation of ICSs' role in international terrorism. To reach this conclusion, I reviewed every published opinion in which Facebook invoked Section 230, ISIS's use of social media and Facebook's counterterrorism efforts, and all recent congressional efforts to repeal or reform Section 230.

Thus, this Note's contribution is that its evaluation of Section 230 is grounded in the law's practical consequences rather than normative assumptions about what Section 230 is or should be. Indeed, most evaluations of Section 230 fail to acknowledge that the law itself is not an ideological proposition ("a free and open internet") or representative of a set of values (capitalism, censorship). Instead, it is an affirmative defense to litigation that has expanded beyond its intended scope through decades of judicial interpretation. Accordingly, this Note will proceed as follows: (I) an overview of Section 230 and its legislative history, (II) a review of Facebook's Section 230 lawsuits, (III) a discussion of ISIS's use of social media and Facebook's counterterrorism efforts, and finally, (IV) an evaluation of two types of legislation currently aimed at reforming Section 230.

I. A General Overview of Section 230

In 1996, Congress passed the Communications Decency Act (CDA), formally Title V of the Telecommunications Act of 1996.[25] For decades, the Telecommunications Act has served as the primary mechanism for regulating

www.wired.com/story/section-230-internet-sacred-law-false-idol/ [https://perma.cc/FLS9-4L43]; Sara Morrison, *Section 230, the Internet Free Speech Law Trump Wants to Repeal, Explained*, VOX (Oct. 6, 2020, 1:19 PM), https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-trump-social-media-twitter-facebook [https://perma.cc/E4P4-PJFA].

22. *See* Katharine Swindells & Laurie Clark, *Big Tech Lobbying: The US Bills Tech Giants Targeted in 2020*, TECHMONITOR (Feb. 15, 2021), https://techmonitor.ai/boardroom/big-tech-lobbying-2020 [https://perma.cc/UY8Q-R9Y9] (explaining Big Tech's monetary expenditures).

23. *See, e.g.*, Edelman, *supra* note 21.

24. *See, e.g.*, VALERIE C. BRANNON, ERIC N. HOLMES, NINA M. HART & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10484, UPDATE: SECTION 230 AND THE EXECUTIVE ORDER ON PREVENTING ONLINE CENSORSHIP 3 (2020).

25. 47 U.S.C. § 609.

the United States telecommunication industry.[26] For its part, the CDA was passed to address growing concerns that minors would have access to pornography on the internet.[27] Section 230 is a subsection of the CDA[28] that provides ICSs with an affirmative defense for civil liability arising from user-generated content.[29] Practically speaking, this means that ICSs cannot be held liable for user-generated content on their platforms.[30] Notably, the inverse is true as well: ICSs cannot be sued for decisions to remove user-generated content.[31]

This protection emerged in response to judicial decisions related to classifying ICSs as distributors or publishers of information.[32] Supreme Court precedent was clear: a line was drawn between publishers of content (like newspapers) and distributors of content (like libraries).[33] Publishers were expected to have an awareness about, and a high degree of control over, the content of material they were publishing and, therefore, were liable for any illegal content they published.[34] Conversely, distributors were less likely to be aware or in control of content and, therefore, were immune from liability arising from the materials they sold.[35]

In the early 1990s, two significant lawsuits sought to impose liability on ICSs: *Cubby, Inc. v. CompuServe Inc*.[36] and *Stratton Oakmont, Inc. v. Prodigy Services Co.*[37] The basis of each lawsuit was the same: the defendant ICSs in those cases were sued for user-generated content hosted on their

26. Richard Adler, *Will the Telecommunications Act Get a Much-Needed Update as It Turns 21?*, VOX (Feb. 8, 2017, 9:05 AM), https://www.vox.com/2017/2/8/14500978/telecommunications-act-1996-regulation-update-telecom-policy [https://perma.cc/8ENP-HU2Z].

27. William A. Sodeman, *Communications Decency Act*, ENCYC. BRITANNICA (Nov. 24, 2016), https://www.britannica.com/topic/Communications-Decency-Act [https://perma.cc/LX7R-SN5R].

28. 47 U.S.C. § 230.

29. Eric Taubel, *The ICS Three-Step: A Procedural Alternative for Section 230 of the Communications Decency Act and Derivative Liability in the Online Setting*, 12 MINN. J.L., SCI. & TECH. 365, 376–77 (2011).

30. VALERIE C. BRANNON, ERIC N. HOLMES, NINA M. HART & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10484, UPDATE: SECTION 230 AND THE EXECUTIVE ORDER ON PREVENTING ONLINE CENSORSHIP 1 (2020).

31. *Id.* at 2.

32. Adi Robertson, *Why the Internet's Most Important Law Exists and How People Are Still Getting It Wrong*, VERGE (June 21, 2019, 1:02 PM), https://www.theverge.com/2019/6/21/18700605/section-230-internet-law-twenty-six-words-that-created-the-internet-jeff-kosseff-interview [https://perma.cc/4FH7-QZET].

33. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020) (mem.) (Thomas, J., statement) (explaining that Congress adopted Section 230 against the backdrop of law that distinguished between publishers and distributors).

34. *Id.*

35. *See* Smith v. California, 361 U.S. 147, 153 (1959) (explaining that booksellers should not be liable for unknowingly selling obscene materials because it would unduly burden booksellers and restrict the public's access to constitutionally protected works).

36. 776 F. Supp. 135 (S.D.N.Y. 1991).

37. No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

websites.[38] The companies' respective approaches to content moderation, however, were markedly different. CompuServe contracted with a third party to manage how users communicated on its servers,[39] whereas Prodigy employed a team of moderators to check and approve content.[40] Thus, under existing Supreme Court precedent, CompuServe was a distributor,[41] and Prodigy was a publisher.[42]

This arrangement struck Representative Christopher Cox (R-CA) as perverse: "[I]f that rule was going to take hold[,] then the internet would become the Wild West and nobody would have any incentive to keep the internet civil."[43] So, in hopes of creating a legal structure that incentivized content moderation to foster civil online discourse, Representative Cox and then-Representative Ron Wyden (D-OR) drafted a bill that would enable ICSs like Prodigy to moderate content without fear of civil litigation.[44] During the House floor debate, Representative Cox stated:

> We want to make sure that everyone in America has an open invitation and feels welcome to participate in the Internet. But as you know, there is some reason for people to be wary because, as a Time Magazine cover story recently highlighted, there is in this vast world of computer information, a literal computer library, some offensive material, some things in the bookstore, if you will, that our children ought not to see.
>
> As the parent of two, I want to make sure that my children have access to this future and that I do not have to worry about what they might be running into on line. I would like to keep that out of my house and off my computer.[45]

Likewise, Congressman Wyden said: "We are all against smut and pornography, and, as the parents of two small[,] computer-literate children, my wife and I have seen our kids find their way into these chat rooms that make their middle-aged parents cringe."[46] At the time, supporters of Section 230 also thought that keeping ICSs out of court would allow the

38. *Cubby, Inc.*, 776 F. Supp. at 138; *Stratton Oakmont, Inc.*, 1995 WL 323710, at *1.

39. *Cubby, Inc.*, 776 F. Supp. at 137.

40. *Stratton Oakmont, Inc.*, 1995 WL 323710, at *4.

41. *Cubby, Inc.*, 776 F. Supp. at 139–40.

42. *Stratton Oakmont, Inc.*, 1995 WL 323710, at *4.

43. Matt Reynolds, *The Strange Story of Section 230, the Obscure Law That Created Our Flawed, Broken Internet*, WIRED UK (Mar. 24, 2019, 6:00 AM), https://www.wired.co.uk/article/section-230-communications-decency-act [https://perma.cc/99B6-PE48].

44. *Id. But cf. Section 230 Protections*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/bloggers/legal/liability/230 [https://perma.cc/F46Y-MJKD] (noting Section 230 does not bar criminal claims, intellectual property claims, or claims arising under electronic communications privacy law); VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 28 (2021) (noting Section 230 does not bar claims arising under federal sex trafficking statutes).

45. 141 CONG. REC. 22,044–45 (Aug. 4, 1995) (statement of Rep. Cox).

46. *Id.* at 22,045 (statement of Rep. Wyden).

fledgling internet to become economically viable.[47] Thus, Section 230 reads: "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."[48]

Undoubtedly, Section 230 has accomplished some of its original goals: now, most major ICSs engage in content moderation and do not face civil liability for doing so.[49] Additionally, ICSs are economically viable: in 2018, the internet sector generated 10.1% of U.S. GDP, created or supported over 19 million jobs, and invested over $60 billion into the economy.[50] Indeed, every American seems to have an "open invitation" to the internet, which over 93% of people in the United States regularly access.[51] Conversely, Section 230 has not been successful in accomplishing at least one of its aims: research suggests children have more access to "smut and pornography" than ever before.[52]

In recent years, Section 230 has become a flashpoint in internet-regulation discourse. A bipartisan coalition is calling for its repeal,[53] while first amendment groups such as the ACLU and tech-friendly organizations such as the Electronic Frontier Foundation are fighting to keep it intact.[54] Both chambers of Congress have held hearings about the law;[55] ICS CEOs

47. Felix Gillette & Laurence Arnold, *Why 'Section 230' Is Nub of Fights Over Online Speech*, BLOOMBERG (Feb. 2, 2021, 4:49 PM), https://www.bloomberg.com/news/articles/2021-02-02/why-section-230-is-nub-of-fights-over-online-speech-quicktake [https://perma.cc/BYA4-J6J6].

48. 47 U.S.C. § 230(c)(1).

49. *See* Corynne McSherry, India McKinney & Jillian C. York, *Content Moderation Is a Losing Battle. Infrastructure Companies Should Refuse to Join the Fight*, ELEC. FRONTIER FOUND. (Apr. 1, 2021), https://www.eff.org/deeplinks/2021/04/content-moderation-losing-battle-infrastructure-companies-should-refuse-join-fight [https://perma.cc/986U-E8SR] (discussing ICSs' efforts to moderate content and explaining that moderation is legally permissible).

50. Christopher Hooton, *Measuring the U.S. Internet Sector: 2019*, INTERNET ASS'N (Sept. 26, 2019), https://internetassociation.org/publications/measuring-us-internet-sector-2019/ [https://perma.cc/Z59U-AYG3].

51. *Internet/Broadband Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband [https://perma.cc/5JXP-DFWL].

52. *See Social Media, Mobile Phones and Sexting*, INTERNET SAFETY 101, https://internetsafety101.org/mobilestatistics [https://perma.cc/7CJY-4VB9] (explaining various ways children access sexual content online and via their mobile phones).

53. Lerman, *supra* note 19.

54. *See, e.g.*, *Communications Decency Act Section 230*, ACLU, https://www.aclu.org/issues/free-speech/internet-speech/communications-decency-act-section-230 [https://perma.cc/MNT7-4EFU]; *Section 230 Protections*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/bloggers/legal/liability/230 [https://perma.cc/Z896-WSAA].

55. Russell Brandom, *Mark Zuckerberg Proposes Limited 230 Reforms Ahead of Congressional Hearing*, VERGE (Mar. 24, 2021, 11:20 AM), https://www.theverge.com/2021/3/24/22348238/zuckerberg-dorsey-pichai-section-230-hearing-misinformation [https://perma.cc/58QJ-NJXF].

have testified to its efficacy;[56] and thousands of articles, podcasts, and online discussion forums are dedicated to discussing Section 230.[57]

Without a doubt, Section 230 is at the heart of the internet regulation zeitgeist. However, most academic, legislative, and media treatment of Section 230 does not consider its practical effects beyond initial acknowledgments that the law protects ICSs from civil suits arising from user-generated content. Section 230 case law is rarely discussed.

By examining the causes of action that Section 230 bars, however, policymakers can make more informed decisions about reforming the law. Put another way, one cannot answer normative questions about updating or refining Section 230 without considering how the law interferes with other statutory and societal objectives.[58] And although there may be hundreds of lenses worthy of such consideration, Part II will advance suggestions for reforming Section 230 through an evaluation of Facebook's Section 230 case law, with a particular focus on cases arising under the Anti-Terrorism Act (ATA).

II. Facebook's Historical Invocation of Section 230 from 2011 to 2021

Since the CDA's passage in 1996, 888 published lawsuits implicating Section 230 have arisen in both state and federal courts.[59] Facebook, and occasionally Facebook CEO Mark Zuckerberg in his personal capacity,[60]

56. *See, e.g.*, *Hearing on Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation Before the Subcomm. on Commc'n & Tech. and the Subcomm. on Consumer Prot. & Com. of the H. Comm. on Energy and Com.*, 117th Cong. (2021) (written testimony of Jack Dorsey, CEO of Twitter), https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-Bio-DorseyJ-20210325.pdf [https://perma.cc/ZQ8D-L6S8]; *id*. (written testimony of Sundar Pichai, CEO of Alphabet), https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-Wstate-PichaiS-20210325-SD001.pdf [https://perma.cc/42BN-MNBC]; *id.* (written testimony of Mark Zuckerberg, CEO of Facebook), https://docs.house.gov/meetings/IF/IF16/20210325/111407/HHRG-117-IF16-Wstate-ZuckerbergM-20210325-U1.pdf [https://perma.cc/9WQQ-PFB8].

57. *See, e.g.*, Lerman, *supra* note 19.

58. For example, is Facebook's freedom to allow users to "troll" more important than the privacy of parents who lost their children to gun violence? Ben Collins, *After Years of 'Crisis Actor' Smears, Sandy Hook Conspiracy Targets Ask Facebook for 'Seat at The Table'*, NBC NEWS (July 19, 2018, 3:46 PM), https://www.nbcnews.com/tech/tech-news/after-years-crisis-actor-smears-sandy-hook-conspiracy-targets-ask-n892926 [https://perma.cc/B5WA-W3Q3]. Is Facebook's First Amendment right to remove content on its platform less worthy of protection given its unprecedented capacity to censor political speech? Sean Illing, *The First Amendment Has a Facebook Problem*, VOX (May 5, 2021, 3:28 PM), https://www.vox.com/policy-and-politics/22356339/free-speech-facebook-twitter-big-tech-first-amendment [https://perma.cc/J8QG-UMNP]. This Note will not attempt to answer these questions, but they are examples of what is at stake in the broader, normative conversation.

59. This number was ascertained from a search in the Westlaw legal database.

60. Discussion of "Facebook" encompasses cases where Zuckerberg was sued in a personal capacity.

have been named defendants in only forty-nine of these cases.[61] However, some of these cases were appeals from lower courts, so, in total, Facebook has faced thirty-four unique plaintiffs in publicly accessible Section 230 decisions—only one has succeeded.[62]

A substantive review of these cases suggests that international terrorism with a social media nexus is not meaningfully addressed in courts. There are two reasons for this. First, as long as Section 230 is in place, the platform will not be held accountable for most harm that arises on the site. Second, even if Section 230 is repealed and replaced with a law that subjects ICSs to civil liability, plaintiffs will likely be unable to establish claims involving international terrorism due to the difficulty of proving proximate causation in such cases.

This section will illustrate the points mentioned above by proceeding with the following: (A) a discussion of Facebook's first and only Section 230 loss: *Fraley v. Facebook*;[63] (B) an overview of the various types of cases in which Facebook routinely invokes Section 230; and (C) a close look at cases involving Facebook's use of Section 230 in the international-terrorism context.

A. Fraley v. Facebook

Facebook's sole loss in a Section 230 case was in one of the first cases in which the company invoked the defense.[64] In *Fraley*, users challenged Facebook's "Sponsored Stories," an advertising service, which was enabled for all members by default.[65] A Sponsored Story would appear on a user's feed and generally consisted of a "Friend's name, profile picture, and an assertion that the person 'like[d]' the advertiser."[66] Sponsored Stories were generated whenever a member used "the Post, Like, or Check-in features" or used an application or played a game within Facebook's website, and the content related "to an advertiser in some way determined by Facebook."[67] Users could not opt out of this feature and alleged that Facebook misappropriated their likeness in violation of California law.[68] In its defense,

61. *See supra* note 59.

62. Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 802–03 (N.D. Cal. 2011) (finding Section 230 did not bar plaintiffs' claim because Facebook's "Sponsored Stories" advertising service involved the company's own editorial choice made for financial gain).

63. 830 F. Supp. 785 (N.D. Cal. 2011).

64. *See generally* Elizabeth Banker, *A Review of Section 230's Meaning and Application Based on More Than 500 Cases*, INTERNET ASSOCIATION, https://internetassociation.org/wp-content/uploads/2020/07/IA_Review-Of-Section-230.pdf [https://perma.cc/XAT6-FE2Q] (reviewing over 500 cases that considered Section 230).

65. *Fraley*, 830 F. Supp. at 791.

66. *Id.*

67. *Id.*

68. *Id.* at 792.

Facebook invoked Section 230 and insisted that "[p]laintiffs themselves provided the information content at issue" and cited "various cases for the blanket proposition that the 'CDA immunity encompasses all state statutory and common law causes of action,' including 'claims alleging misappropriation of name and likeness.'"[69] The court found, however, that although ICSs were entitled to broad immunity for content published by third parties, the plaintiffs were entitled to recover because they did not allege Facebook was publishing tortious content.[70] Instead, they claimed it was affirmatively developing "commercial content that violate[d] their statutory right of publicity."[71]

After *Fraley*, Facebook enabled users to opt out of features that might be considered commercial content,[72] and no similar suits have arisen. Since 2011, no plaintiff has recovered in any court, state or federal, where Facebook has invoked Section 230 regardless of the behavior alleged. In each instance, courts, particularly the Northern District of California, which has considered the most cases involving Section 230, have adopted a broad interpretation of ICSs' protection from civil claims.[73]

B. Other Lawsuits

Since 2011, and particularly as of late, litigation against Facebook has picked up.[74] However, the cases in which the company invokes Section 230 stand out; largely, this is because of the contrast between varying degrees of the harm alleged and the singularity of the results. While some claimants sought to recover after nominal instances of defamation,[75] others sought to recover after murders and mass shootings.[76] Further, some claimants asserted

69. *Id.* at 801.

70. *Id.*

71. *Id.*

72. *See Fraley v. Facebook*, PUB. CITIZEN, https://www.citizen.org/litigation/fraley-v-facebook-6/ [https://perma.cc/S4L6-XUEB] (explaining that the settlement agreement in *Fraley v. Facebook* required that Facebook create a mechanism for users to opt out of Sponsored Stories).

73. *See infra* notes 76–97 (citing cases in which Facebook won using the Section 230 affirmative defense).

74. *See, e.g.*, *U.S. Government, States Ask Judge to Deny Facebook's Request to Dismiss Lawsuits*, REUTERS (Apr. 8, 2021, 2:06 AM), https://www.reuters.com/article/us-tech-antitrust-facebook/u-s-government-states-ask-judge-to-deny-facebooks-request-to-dismiss-lawsuits-idUSKBN2BV06P [https://perma.cc/DZ8Q-25AD]; *FTC Sues Facebook for Illegal Monopolization*, FED. TRADE COMM'N (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization [https://perma.cc/Y8Q8-6FRL]; Associated Press, *Judge Approves $650m Settlement of Privacy Lawsuit Against Facebook*, THE GUARDIAN (Feb. 27, 2021, 8:36 AM), https://www.theguardian.com/technology/2021/feb/27/facebook-illinois-privacy-lawsuit-settlement [https://perma.cc/TE5M-ZVZK].

75. *See, e.g.*, Igbonwa v. Facebook, Inc., No. 18-CV-02027, 2018 WL 4907632, at *1 (N.D. Cal. Oct. 9, 2018), *aff'd*, 786 Fed. App'x 104 (9th Cir. 2019).

76. *See, e.g.*, Godwin v. Facebook, Inc., 160 N.E.3d 372, 375 (Ohio Ct. App. 2020) (involving a murder); Crosby v. Twitter, Inc., 921 F.3d 617, 619 (6th Cir. 2019) (involving a mass shooting).

Facebook failed to take action and, thus, caused harm,[77] while others suggested the company directly participated in the incidents that prompted their lawsuits.[78] Yet, no matter the form or substance of the underlying allegation, the result was always the same: Facebook won.

Generally, the CDA has been interpreted to mean that Facebook is immunized from liability because:

> (i) Facebook is a "provider or user of an interactive computer service," (ii) the information for which the [plaintiff sought] to hold Facebook liable was "information provided by another information content provider," and (iii) the [plaintiff's claim sought] to hold Facebook liable as the "publisher or speaker" of that information.[79]

Generally speaking, Facebook's Section 230 case law can be characterized in two ways: cases arise from either (1) Facebook's inaction or (2) its direct action. Thus, the following sections are meant to illustrate this distinction for the purpose of giving readers insight into the breadth of Section 230's protections. Practitioners, policymakers, and academics will have flawed discussions and, therefore, reach flawed conclusions about reforming Section 230 if they fail to consider a holistic survey of the law's operation. That is, addressing problems posed by Section 230 in one context might produce unfortunate, unanticipated outcomes in other contexts if particular types of Section 230 cases are assessed in isolation.

1. Cases Arising from Facebook's Inaction.—The majority of cases in which Facebook's inaction prompted suit were instances where it failed to remove defamatory comments or images. For example, one plaintiff alleged Facebook failed to reveal the identities behind accounts posting content suggesting the plaintiff engaged in illegal or scandalous behavior.[80] Another asserted Facebook failed to remove pictures of an arrest.[81] Facebook's alleged inaction also led to severe harm in other types of incidents—some

77. *See*, *e.g.*, Jefferson v. Zuckerberg, No. RDB-17-3299, 2018 WL 3241343, at *1 (D. Md. July 3, 2018) (alleging failure to remove pictures of claimant's arrest).

78. *See*, *e.g.*, Shulman v. Facebook.com, No. 17-764, 2017 WL 5129885, at *2 (D.N.J. Nov. 6, 2017) (alleging suppression of political speech).

79. Klayman v. Zuckerberg, 753 F.3d 1354, 1357 (D.C. Cir. 2014) (quoting 47 U.S.C. § 230(c)(1)); *see also* Sikhs for Justice, Inc. v. Facebook, Inc., 144 F. Supp. 3d 1088, 1092–93 (N.D. Cal. 2015) (citing 47 U.S.C. § 230(c)(1)).

80. *Igbonwa*, 2018 WL 4907632, at *1 (alleging anonymous accounts posted falsehoods about the plaintiff "'rang[ing] from criminal activities that never took place to falsehoods about Plaintiff's personal life,' and include[d] allegations that he is a money-launderer, a wife beater and a 'scammer.'").

81. *Jefferson*, 2018 WL 3241343, at *1.

plaintiffs were victims of revenge porn,[82] hate speech,[83] and sex trafficking.[84] In one case, the estate of an individual whose murder was broadcast via "Facebook Live" attempted to recover pain and suffering damages for Facebook's failure to warn the victim of the murderer's ill intentions that were posted to Facebook on the day of the murder.[85] Notably, at least one plaintiff brought a negligence claim alleging that Facebook's failure to remove advertisements commercially benefited the site.[86] In 2019, a Philadelphia news anchor sued Facebook because it failed to prevent third parties from disseminating advertisements to "meet and chat with local single women" featuring her likeness.[87] All of the aforementioned claims were barred by Section 230 because courts determined third parties caused harm while using Facebook but that Facebook itself did not cause the harm.[88]

2. Cases Arising from Facebook's Affirmative Actions.—Still, other claims allege harm that resulted from Facebook's direct action. For example, one lawsuit suggested that Facebook removed a plaintiff's account because it "regularly conspire[s] . . . to oppress opposing opinions and freedom of speech to dissent with respect to their flooding their own opinions, facts or false facts and News on the public."[89] Like the claims alleging inaction, claims alleging direct action also occasionally featured plaintiffs that suffered from more severe kinds of harm. For example, in *Vargas v. Facebook*,[90] the plaintiffs claimed Facebook's self-selecting advertising tools facilitated housing discrimination in violation of the federal Fair Housing Act.[91]

In these "direct action" cases, claimants also implied Facebook was exploiting Section 230's protection to gain a commercial advantage. In *Fyk v. Facebook, Inc.*,[92] a content creator claimed that Facebook suppressed traffic to his pages and unpublished or otherwise restricted various posts on his pages, which had over 25 million followers, because he did not use

82. Sekiya v. Zuckerberg, No. 17CV283, 2017 WL 3405627, at *2 (D.N.M. Mar. 10, 2017) (alleging Facebook failed to remove an account created by the plaintiff's ex-boyfriend, who friended the plaintiff's "Friends" and featured nude photos of the plaintiff).

83. La'Tiejira v. Facebook, Inc., 272 F. Supp. 3d 981, 988–90 (S.D. Tex. 2017) (alleging Facebook allowed a user to target a transgender individual with hate speech).

84. *In re* Facebook, Inc., 625 S.W.3d 80, 84–85 (Tex. 2021) (alleging Facebook allowed the plaintiffs to be sex trafficked).

85. Godwin v. Facebook, Inc., 160 N.E.3d 372, 375 (Ohio Ct. App. 2020).

86. Hepp v. Facebook, Inc., 465 F. Supp. 3d 491, 495 (E.D. Pa. 2020).

87. *Id.* at 494–95.

88. *See, e.g.*, *id.* at 489–99 (finding that the defendants met the criteria for immunity under Section 230).

89. Shulman v. Facebook.com, No. 17-764, 2017 WL 5129885, at *2 (D.N.J. Nov. 6, 2017).

90. Vargas v. Facebook, Inc., No. 19-CV-05081, 2021 WL 214206 (N.D. Cal. Jan. 21, 2021).

91. *Id.* at *1.

92. No. C 18-05159, 2019 WL 11288576 (N.D. Cal. June 18, 2019), *aff'd*, 808 Fed. App'x 597 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1067 (2021).

Facebook's paid advertising services.[93] As a result, the creator sold his pages to a competitor that had previously spent $22 million on Facebook advertising.[94] Subsequently, Facebook re-published and unrestricted the previously suppressed content.[95] On these facts, the District Court for the Northern District of California found Section 230 barred the creator's claim because there was "no dispute that Plaintiff was the sole creator of his own content,"[96] and the Ninth Circuit affirmed because "[t]hat Facebook allegedly took its actions for monetary purposes does not somehow transform Facebook into a content developer."[97] Indeed, since *Fraley*, courts have refused to interpret Facebook's actions as falling outside of Section 230's protections.

C. Terrorism Lawsuits

Moreover, while all of the cases discussed above demonstrate the breadth of protection Section 230 provides ICSs, Facebook's international-terrorism cases underscore unique challenges. Unlike the cases that involved discrete instances of cyberbullying or defamation, the international-terrorism claims often attempted to hold Facebook responsible for harms that arose from terrorists' systemic use of the platform. These cases involved high-profile incidents of international terrorism, including the Pulse Night Club massacre, the 2015 Paris attacks, and the 2017 Barcelona attack.

All of these cases proceeded on slightly different legal theories, but none of the respective arguments were successful. In total, Facebook has invoked Section 230 in six cases involving international terrorism: *Crosby v. Twitter, Inc.*,[98] *Palmucci v. Twitter, Inc.*,[99] *Retana v. Twitter, Inc.*,[100] *Sinclair ex rel. Tucker v. Twitter, Inc.*,[101] *Cohen v. Facebook, Inc.*,[102] and *Force v. Facebook, Inc.*[103] One set of these cases alleges Facebook provides international terrorists with communications platforms, while the other points to Facebook's algorithms as its direct participation in the attacks.

---

93. Brief for Petitioner at 11–12, Fyk v. Facebook, Inc., 141 S. Ct. 1067 (2021) (No. 20-632).

94. *Id.* at 12.

95. Fyk v. Facebook, Inc., 808 Fed. App'x 597, 598 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1067 (2021).

96. *Fyk*, 2019 WL 11288576, at *2.

97. *Fyk*, 808 Fed. App'x at 598.

98. 921 F.3d 617 (6th Cir. 2019).

99. No. 18-CV-03947, 2019 WL 1676079 (N.D. Cal. Apr. 17, 2019).

100. 419 F. Supp. 3d 989 (N.D. Tex. 2019), *aff'd*, 1 F.4th 378 (5th Cir. 2021).

101. No. C 17-5710, 2019 WL 10252752 (N.D. Cal. Mar. 20, 2019).

102. 252 F. Supp. 3d 140 (E.D.N.Y. 2017), *aff'd in part, dismissed in part sub nom.* Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019).

103. 934 F.3d 53 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020). While some of the case headings are stylized as "Plaintiff v. Twitter," Facebook was also a defendant.

Both categories, however, underscore two key insights into possible Section 230 reform. First, and most obviously, Section 230 prevents plaintiffs from bringing cases under the Anti-Terrorism Act (ATA), which sets out a civil cause of action against individuals and corporations that provide material assistance to terrorists. Second, neither repealing nor amending Section 230 would make these plaintiffs more successful. Specifically, even if plaintiffs' claims were not barred by Section 230, under existing common law precedent they cannot establish that Facebook proximately caused their injuries. Further, a law that creates liability for harm caused by international terrorism will merely relocate line-drawing problems that exist under Section 230. That is, if a new liability carveout permits individuals to bring suit against ICSs for their roles in acts of international terrorism, the law will still leave every other type of harm with a one-size-fits-all bar.

Thus, if policymakers seek to impose this particular sort of liability on ICSs, which seems likely given that the statute was written to apply to all corporations, simply removing Section 230's protections will not be enough.[104] The following discussion will demonstrate this is true in both cases suggesting Facebook provided terrorists with a communication platform and those in which plaintiffs alleged the company's algorithms constituted direct participation in instances of international terrorism.

1. Anti-Terrorism Act: How to Provide Material Assistance to Terrorists.—Under federal law, international-terrorism consists of violent or dangerous acts that violate federal criminal law and occur outside of the United States or otherwise "transcend national boundaries" in terms of either the means used or the targeted victims.[105] Further, such acts must appear intended to: (1) "intimidate or coerce a civilian population," (2) "influence the policy of a government," or (3) "affect the conduct of a government by mass destruction, assassination, or kidnapping."[106] Those who aid, abet, or provide "material support or resources," such as communications equipment, to international terrorists are subject to civil liability under the ATA.[107] Both individuals and companies, like Facebook, are subject to this statute, which

104. If policymakers want plaintiffs to recover, they will need to update statutory causes of action to encompass broader forms of directness in the context of civil claims involving ICSs. Although it is beyond the scope of this Note to consider what sort of statutory language might address this issue, the cases described below suggest that in order to recover, plaintiffs must be allowed to establish something more attenuated than the current proximate causation standard under the ATA, which requires plaintiffs prove that a particular company "compel[led]" a terrorist attack. Crosby v. Twitter, Inc., 921 F.3d 617, 625 (6th Cir. 2019).

105. 18 U.S.C. § 2331(1).

106. *Id.*

107. *Id.* § 2339A(a); *id.* § 2339A(b)(1).

allows "[a]ny national of the United States" or their estate to recover from harm caused by international-terrorism.[108]

Practically speaking, this definition encompasses events ranging from the highly sophisticated attacks like 9/11 to planned-but-thwarted, lone-wolf shootings.[109] Under the ATA, ICSs could theoretically be held liable for damages arising from acts of terrorism, including attacks that were not planned online but were carried out by individuals who were recruited to join such organizations online.[110] But, as discussed above, Section 230 has been broadly interpreted to preclude ICS's from almost any kind of civil liability that arises from their user's activity.[111] ATA cases are no exception.

Since Section 230's passage, at least 170,000 people have been killed by international terrorist attacks, including 3,905 Americans.[112] None have successfully recovered against an ICS in an ATA suit. Although international terrorism predates the world wide web, the rise of the internet has revolutionized terrorists' ability to plan, connect, and communicate.[113] Thus, Section 230 effectively nullifies the ATA's purpose in precisely the sort of cases it was meant to encompass, i.e., those in which plaintiffs are harmed because corporations have provided valuable services to terrorists.

2. Facilitation of Communications Platforms.—Facebook has faced four cases involving accusations that the platform facilitated terrorists' communication: *Crosby v. Twitter, Inc.*, *Palmucci v. Twitter, Inc.*, *Retana v. Twitter Inc.*, and *Sinclair ex rel. Tucker v. Twitter, Inc.*, which all proceeded

108. *Id.* § 2333(a); *see also* 1 U.S.C. § 1 ("[T]he words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals.").

109. *See, e.g.*, *Cincinnati-Area Man Sentenced to 30 Years in Prison for Attempting Terrorism Plot to Kill Government Employees*, DEP'T JUST. (Dec. 5, 2016), https://www.justice.gov/opa/pr/cincinnati-area-man-sentenced-30-years-prison-attempting-terrorism-plot-kill-government [https://perma.cc/7HCY-2USG] (reporting on the prosecution of a lone-wolf terrorist, who plotted against government employees).

110. Jaime M. Freilich, Note, *Section 230's Liability Shield in the Age of Online Terrorist Recruitment*, 83 BROOK. L. REV. 675, 677–78 (2018).

111. *See, e.g.*, Force v. Facebook, Inc., 934 F.3d 53, 57 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020) (holding that Section 230 barred recovery under ATA in Hamas attacks in Israel).

112. Erin Miller & Michael Jensen, *Fact Sheet, American Deaths in Terrorist Attacks, 1995–2019*, START 1 (Oct. 2020), https://www.start.umd.edu/pubs/START_AmericanTerrorismDeaths_FactSheet_Oct2020.pdf [https://perma.cc/JF8H-F3BJ]; Crime and Law Enforcement, *Number of Fatalities Due to Terrorist Attacks Worldwide Between 2006 and 2019*, STATISTA, https://www.statista.com/statistics/202871/number-of-fatalities-by-terrorist-attacks-worldwide/ [https://perma.cc/MAF2-VEVY].

113. *See* Mitchell D. Silber & Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, CITY N.Y. POLICE DEP'T 83 (2007), http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf [https://perma.cc/N3A4-ZYPU] ("The Internet is a driver and enabler for the process of radicalization."). This point will be discussed in further detail in subpart III(A).

on roughly the same grounds. First, *Crosby v. Twitter* arose from the Pulse Night Club massacre in which an ISIS-inspired shooter opened fire in a Florida nightclub and killed forty-nine people.[114] Here, plaintiffs filed suit under the Anti-Terrorism Act (ATA), claiming that ISIS used Facebook "to post propaganda and 'virtually recruit' Americans to commit terrorist attacks."[115] Plaintiffs further asserted the nightclub shooter was one such recruit: "he allegedly viewed ISIS-related material online [and] became 'self-radicalized.'"[116] In fact, shortly before the attack, the shooter declared allegiance to ISIS on Facebook,[117] and shortly after the massacre, ISIS claimed responsibility.[118]

The plaintiffs' theory of causation was essentially that Facebook facilitated the spread of terrorist content that radicalized the shooter, provided him with a platform to discuss his ideology, and, therefore, caused him to murder dozens of people.[119] The court, however, rejected this theory and found that Facebook's role in the shooting was not foreseeable, direct, or enough of a substantial factor in the attack to satisfy proximate causation under the ATA.[120]

More specially, the *Crosby* court noted that the ATA currently enables "recovery [for] injuries sustained 'by reason of an act of international terrorism,'"[121] and "[t]he Supreme Court has repeatedly and explicitly held that when Congress uses the phrase 'by reason of' in a statute, it intends to require a showing of proximate cause."[122] The court then adapted the D.C. and Second Circuits' test for proving proximate causation under the ATA:

> [T]he Second Circuit's two-part test for proximate cause under the ATA [is]: (1) whether the defendants' acts were "a 'substantial factor' in the sequence of events" that led to the plaintiffs' injuries; and (2) whether those injuries were "reasonably foreseeable or anticipated as a natural consequence of" defendants' conduct. In a footnote, the [D.C. Circuit] explained how this test fits with a "direct relation" test. A proximate cause test that requires defendants' conduct to be "'a substantial factor in the sequence of responsible causation' likewise requires sufficient directness." Said another way, substantiality,

114. 921 F.3d 617, 619 (6th Cir. 2019).

115. *Id.*

116. *Id.*

117. *Id.* at 621.

118. Jared Malsin, *What to Know About ISIS's Role in the Orlando Shooting*, TIME (June 13, 2016, 6:30 AM), https://time.com/4365507/orlando-shooting-isis-claims-responsibility-terror/ [https://perma.cc/79CU-HJAE].

119. *Crosby*, 921 F.3d at 619.

120. *Id.* at 626.

121. *Id.* at 623 (emphasis omitted) (quoting 18 U.S.C. § 2333(a)).

122. *Id.* (quoting Kemper v. Deutsche Bank AG, 911 F.3d 383, 391 (7th Cir. 2018)).

> directness, and foreseeability are all relevant in a proximate cause determination.[123]

On this test, the court noted that plaintiffs' theory was "tenuous . . . at best" because they merely alleged that "at some point before the Pulse Night Club shooting, [the terrorist] viewed online content from ISIS and became 'self-radicalized.'"[124] Although the court acknowledged that the interconnected nature of social media would cause "ripples of harm," it noted such ripples "flow[ed] far beyond the defendant's misconduct."[125] Thus, the plaintiff failed to establish proximate causation under the ATA because Facebook's "content did not *compel* the terrorist's actions."[126]

In *Palmucci v. Twitter, Inc.*, the plaintiff embraced a similar theory of causation in her suit to recover for personal injuries she suffered during the 2015 Paris attacks, where ISIS shooters killed over 130 people and injured more than 400 others.[127] Specifically, she sought to establish that Facebook profited by allowing ISIS to use its services through advertisements placed on ISIS posts.[128] She claimed that "because ISIS content [wa]s shown on defendants' sites with 'configured' ads provided by defendants, defendants not only profit[ed] from ISIS content on their sites but [we]re also 'content providers."[129] Like the court in *Crosby*, the *Palmucci* court found the plaintiff could not establish proximate causation under the ATA.[130] Specifically, it noted that plaintiff pleaded "no facts indicating that [the] attack was in any way impacted, helped by, or the result of ISIS's presence on the social network."[131]

In *Retana v. Twitter, Inc.*, a court in the Northern District of Texas cited *Crosby* to reach the same result where a police officer and his husband alleged that defendants (Twitter, Facebook, and Google) hosted content that supported Hamas's activities in Israel, which, in turn, inspired a lone-wolf shooting in Dallas.[132] On appeal, plaintiffs insisted that the correct test for proximate causation required that the "alleged injuries proximately flow from the principal's terrorist attack, not the secondary actor's supportive conduct."[133] The Fifth Circuit noted that even that standard required plaintiffs

123. *Id.* at 624 (citations omitted) (quoting Owens v. BNP Paribas, S.A., 897 F.3d 266 (D.C. Cir. 2018)).

124. *Id.* at 625.

125. *Id.* (quoting Fields v. Twitter, Inc., 881 F.3d 739, 749 (9th Cir. 2018)).

126. *Id.*

127. Palmucci v. Twitter Inc., No. 18-CV-03947, 2019 WL 1676079, at *1 (N.D. Cal. Apr. 17, 2019).

128. *Id.*

129. *Id.*

130. *Id.* at *3.

131. *Id.* at *2–3 (quoting Fields v. Twitter, Inc., 881 F.3d 739, 750 (9th Cir. 2018)).

132. 419 F. Supp. 3d 989, 991–92, 999 (N.D. Tex. 2019), *aff'd*, 1 F.4th 378 (5th Cir. 2021).

133. Retana v. Twitter, Inc., 1 F.4th 378, 384 (5th Cir. 2021).

to prove that Hamas played a role in the Dallas shooting, which they failed to do because the group claimed no responsibility for (or knowledge of) the attack.[134]

Likewise, in *Sinclair ex rel. Tucker*, a court in the Northern District of California reached the same result where the plaintiffs were the children of an individual who died after an ISIS fighter ran a van through a crowd on a busy street in Barcelona.[135] Plaintiffs alleged that Facebook and the other named defendants were "responsible for the Barcelona Attack by virtue of allowing ISIS to utilize their respective social media platforms to recruit, fund[,] and encourage terrorist attacks."[136] "The pleadings d[id] not allege that ISIS used social media to direct the Barcelona Attack," but rather that the individual fighter "was radicalized by ISIS's use of social media" and "thereafter carried out the attack."[137] As in *Crosby*, *Palmucci*, and *Retana*, the *Sinclair* court found the plaintiff's claims were "devoid of any facts demonstrating a direct relationship between Defendants' conduct (i.e., hosting ISIS's content) and the attack that killed the [d]ecedent."[138] The court went on to suggest that even if it accepted plaintiff's theory:

> No facts are alleged that ISIS used any particular social media platform—including those operated by Defendants—to direct its members or others to carry out the Barcelona Attack. Nor are any facts alleged that Abouyaaqoub, in fact, personally viewed any of ISIS's materials on-line, let alone that he did so using Defendants' social media platforms. Although ISIS claimed responsibility for the attack after it occurred, courts have rejected the notion that a post-attack claim of responsibility is sufficient to satisfy the direct relationship standard of proximate causation.[139]

Thus, from these cases we can discern that even if Section 230 were repealed entirely, plaintiffs could not recover from ICSs under the ATA where their claims turn on terrorists' radicalization via social media platforms. Perhaps this was Congress's intention: maybe it is socially undesirable to impose civil liability in this context. But, even if it is, a few facts remain. First, terrorists are radicalized on social media platforms, and many have committed deadly attacks. Second, social media platforms are aware of this and attempt to moderate terrorist content and accounts.[140] Third,

134. *Id.*

135. Sinclair *ex rel.* Tucker v. Twitter, Inc., No. C 17-5710, 2019 WL 10252752, at *1 (N.D. Cal. Mar. 20, 2019).

136. *Id.* at *2.

137. *Id.*

138. *Id.* at *4.

139. *Id.* (citing Clayborn v. Twitter, Inc., No. 17-CV-06894, 2018 WL 6839754, at *7 (N.D. Cal. 2018)).

140. *See infra* note 181–186 and accompanying text.

there are currently no legal or regulatory mechanisms that hold ICSs to particular standards of conduct or provide accountability when platforms have clearly failed to self-regulate.

3. Cohen v. Facebook *and* Force v. Facebook.—*Cohen* and *Force* were separate cases that were consolidated as *Force v. Facebook*.[141] In *Force*, the estates of victims and one survivor of Hamas-instigated attacks brought claims under the ATA and the Justice Against Sponsors of Terrorism Act.[142] The plaintiffs also cited to 18 U.S.C. § 2339B(a)(1),[143] which provides a civil cause of action against any person or organization that "knowingly provides material support or resources to a foreign terrorist organization,"[144] where material assistance includes "communications equipment."[145] Because Hamas is a recognized terrorist organization, the plaintiffs advanced two theories about how Facebook materially assisted the organization.[146]

First, like the cases outlined above, *Force* claimed that "Facebook assisted Hamas by providing Hamas and its operatives with a communications platform, consisting of a Facebook page on which Hamas could post statements, photographs, videos, and information about events."[147] However, unlike plaintiffs in *Crosby*, *Palmucci*, *Retana*, and *Sinclair*, the *Force* plaintiffs alleged Facebook took "several affirmative steps" that "materially assisted Hamas." These included: (1) recommending content like photographs, videos, and statements that Hamas "posted on its Facebook page"; (2) notifying "other Facebook users of events sponsored by Hamas"; and (3) recommending to users, "'friend' . . . the Hamas Facebook page, all of which" might generate notifications from Facebook and lead users to Hamas statements and other content.[148]

Facebook asserted these claims were barred by Section 230 because they turned on Facebook's editorial discretion.[149] Accordingly, the district court judge sitting in the Eastern District of New York and the three-judge panel at the Second Circuit dismissed the plaintiffs' claims on those grounds.[150]

141. Force v. Facebook, Inc., 934 F.3d 53, 53 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

142. *Id.* at 58, 62.

143. *Id.* at 61 n.10.

144. 18 U.S.C. § 2339B.

145. *Id.* § 2339A(b)(1).

146. *Force*, 934 F.3d at 61.

147. Brief for the Petitioner at 10, Force v. Facebook, Inc., 140 S. Ct. 2761 (2020) (No. 19-859).

148. *Id.* at 11–12.

149. *Force*, 934 F.3d at 57.

150. *Id.*

However, Chief Judge Robert Katzmann dissented from the Section 230 portion of the opinion.[151] In his dissent, Judge Katzmann found that "it strains the English language to say that in targeting and recommending these writings to users—and thereby forging connections, developing new social networks—Facebook is acting as 'the publisher of . . . information provided by another information content provider.'"[152] He also noted, "plaintiff[s] bring[] a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals[;] the CDA does not and should not bar relief."[153] However, that is precisely the broad interpretation of Section 230 embraced by courts across the country. Nevertheless, *Force* and a companion case, *Dyroff v. Ultimate Software Group, Inc.*,[154] were denied certiorari last year.[155]

III. Practical Case Studies: ISIS's Use of Social Media and Facebook's Counterterrorism Efforts

Judge Katzman's dissent seems particularly right-headed in the anti-terrorism context. Indeed, social media has been ISIS's "most powerful weapon" since the organization's founding precisely because of the connections platforms enable.[156] Thus, the ensuing subparts will support Katzmann's commentary and the need for proactive internet regulation by discussing ISIS's use of social media and Facebook's approach to counterterrorism.

A. Social Media, ISIS's Most Powerful Weapon

Former FBI Director James Comey has noted that even if we were able to keep foreign terrorists physically out of the United States, online communication and social media allow ISIS to "enter as a photon and radicalize somebody in Wichita, Kansas."[157] As Senator Rob Portman (R-OH), then-Chairman of the Senate Permanent Subcommittee on

151. *Id.* at 76 (Katzmann, C.J., dissenting).

152. *Id.* at 76–77 (emphasis omitted).

153. *Id.* at 77.

154. 934 F.3d 1093 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

155. Adi Robertson, *Supreme Court Rejects Lawsuit Against Facebook for Hosting Terrorists*, VERGE (May 18, 2020, 11:30 AM), https://www.theverge.com/2020/5/18/21262248/supreme-court-rejects-stuart-force-facebook-section-230-lawsuit-algorithms [https://perma.cc/UNN6-BYNC].

156. Kai Ryssdal, *The Internet Is ISIS' Most Powerful Weapon*, MARKETPLACE (July 1, 2016), https://www.marketplace.org/2016/07/01/isis-s-most-powerful-weapon-internet/ [https://perma.cc/FW8M-PHG9].

157. Brent Kendall & Jay Solomon, *FBI Cites Online Terror Recruiting, Training, Damps Subway-Plot Claim*, WALL ST. J. (Sept. 25, 2014, 2:46 PM), https://www.wsj.com/articles/fbi-director-cites-online-terror-recruiting-training-damps-subway-plot-claim-1411688762 [https://perma.cc/4VLV-Z43T].

Investigation, similarly stated, "ISIS has weaponized online propaganda in a new and very lethal way."[158]

Several foreign and domestic institutions have researched the means by which individuals become radicalized and join international terrorist organizations. Historically, groups like Al Qaeda gained a significant portion of their membership from localized recruiting efforts and by absorbing smaller extremist organizations.[159] Likewise, many of ISIS's local recruits fit the demographic profile of traditional terrorist organizations: disenfranchised youth in localities with poor economies and fractured governments, either inspired by older generations of jihadists or enticed by the promise of comradery, resources, and purpose.[160] Some ISIS recruits came from prisons,[161] or preexisting criminal or jihadist networks,[162] while others were drawn to the organization by the group's "certain glamour among urban youth," which stemmed from ISIS's relatively lax religious knowledge and piety membership requirements. [163]

However, the roughly 30,000 foreign fighters who traveled to Syria and Iran to join ISIS mostly came in contact with the group online.[164] These members are especially valuable to the group because they tend to be more willing to engage in high-risk attacks than local recruits and more dedicated to the cause overall.[165] In part, this is because they have little hope of returning to their countries of origin or integrating with old familial ties and, thus, feel they have little to lose.[166] Many of ISIS's most deadly, high-profile attacks, such as the Pulse Night Club massacre in Orlando, the Sri Lanka Easter massacre, and the Fort Hood shootings, were committed by foreign recruits or foreign ISIS sympathizers.[167] All of those terrorists were

158. *ISIS Online Hearing*, *supra* note 12, at 2.

159. Daniel L. Byman, *Al Qaeda's M&A Strategy*, BROOKINGS (Dec. 7, 2010), https://www.brookings.edu/opinions/al-qaedas-ma-strategy/ [https://perma.cc/4RBJ-PLL4].

160. *How the Islamic State Rose, Fell and Could Rise Again in the Maghreb*, INT'L CRISIS GROUP 7, 8 (July 24, 2017), https://d2071andvip0wj.cloudfront.net/178-how-the-islamic-state-rose_0.pdf [https://perma.cc/TED3-W99M]; *cf. id.* at 10 [hereinafter *How the Islamic State Rose*] ("The link between regional marginalisation, poverty, state neglect, petty criminality and jihadist recruitment is not straightforward or direct.").

161. *Id.* at 8.

162. *Id.*

163. *Id.* at 10; *see also* Vera Mironova, *Who Are the ISIS People?*, PERSPS. ON TERRORISM, Feb. 2019, at 32, 33–34 (outlining the reasons that individuals joined ISIS).

164. Tamar Mitts, *From Isolation to Radicalization: Anti-Muslim Hostility and Support for ISIS in the West*, 113 AM. POL. SCI. REV. 173, 173 (2019).

165. Mironova, *supra* note 163, at 33.

166. *Id.*

167. Williams, *supra* note 4; *The Latest: Military Clashes with Suspects in Sri Lanka*, ASSOCIATED PRESS (Apr. 26, 2019), https://apnews.com/article/travel-asia-pacific-religion-suicide-bombings-islamic-state-group-b3eaa2de047e4ef9bcf5755dfb9076d4 [https://perma.cc/

reportedly radicalized (to varying degrees) online, and all of them killed American citizens.[168] Notably, the Sri Lanka massacre was ignited in retaliation for another incident of mass violence that was livestreamed across social media.[169]

ISIS lures foreign fighters in several ways: through Twitter messages, "love bombing," videos on YouTube, and online messaging via Facebook.[170] Love bombing is a practice through which ISIS recruiters contact individuals who engage with ISIS recruitment on social media by liking, retweeting, sharing, or otherwise endorsing ISIS propaganda messages.[171] The practice is effective. In fact, many ISIS members mentioned that videos posted online influenced them to join.[172] One recruit, a twenty-nine-year-old from Belgium, recalled that watching ISIS videos "convinced him that it was his obligation

5YET-W9ZD]; Chelsea J. Carter, *Fort Hood Shooter Writes to ISIS Leader, Asks to Become 'Citizen' of Islamic State*, CNN (Aug. 29, 2014, 11:41 AM), https://www.cnn.com/2014/08/28/us/isis-fort-hood-shooter [https://perma.cc/X8E9-7MRN]. Please note I am drawing a distinction between foreign recruits and foreign sympathizers. For the purposes of this Note, a foreign recruit refers to a foreigner who formally joins ISIS, whereas a foreign ISIS sympathizer refers to someone who carries out attacks without formally joining the group.

168. *See ISIS Online Hearing*, *supra* note 12, at 2 (statement of Sen. Rob Portman (R-OH), Chairman, S. Permanent Subcomm. on Investigations) (explaining that the killers in the Pulse Nightclub massacre and Fort Hood shootings were radicalized online and killed Americans); Joanna Slater & Amantha Perera, *Sri Lankan Spice Tycoon's Sons and Daughter-in-Law Were Suicide Bombers in Easter Attacks*, WASH. POST (Apr. 25, 2019), https://www.washingtonpost.com/world/asia_pacific/sri-lanka-reveals-identities-of-suicide-bombers-behind-easter-massacres/2019/04/24/5df35f60-6611-11e9-a698-2a8f808c9cfb_story.html [https://perma.cc/G5AX-4XYL] (reporting that the leader of the bombings posted online sermons encouraging religious division); Katie Mettler & Michael Brice-Saddler, *A Billionaire's Children, a D.C. Fifth-Grader, a Celebrity Chef: The Victims in Sri Lanka*, WASH. POST (Apr. 23, 2019), https://www.washingtonpost.com/world/2019/04/22/celebrity-chef-children-denmark-billionaire-among-dead-sri-lanka-bomb-attacks [https://perma.cc/YP5P-73HN] (reporting that American citizens were killed in the Sri Lanka Easter massacre).

169. *See* Sanjeev Laxman & Ben Kesslen, *Sri Lanka Bombings Were Retaliation for Christchurch Shooting, Defense Minister Says*, NBC NEWS (Apr. 23, 2019, 1:18 PM), https://www.nbcnews.com/news/world/sri-lanka-bombing-was-retaliation-christchurch-shooting-defense-minister-says-n997391 [https://perma.cc/7D5R-P7PK] (reporting that the Sri Lanka Easter massacre was in retaliation for the New Zealand shootings of a mosque in Christchurch); Alexander Smith, Caroline Radnofsky, Linda Givetash & Vladimir Banic, *New Zealand Mosque Shooting: Attacker's Apparent Manifesto Probed*, NBC NEWS (Mar. 15, 2019, 10:13 AM), https://www.nbcnews.com/news/world/new-zealand-mosque-terrorist-may-have-targeted-country-because-it-n983601 [https://perma.cc/ESQ4-PZXJ] (reporting that the Christchurch shooting was livestreamed on social media). Underscoring the importance of social media in these incidents, blocking social media was among the first protective measures taken by the Sri Lankan government. Laxman, *supra*.

170. *See* Anne Speckhard & Molly D. Ellenberg, *ISIS in Their Own Words: Recruitment History, Motivations for Joining, Travel, Experiences in ISIS, and Disillusionment Over Time—Analysis of 220 In-Depth Interviews of ISIS Returnees, Defectors and Prisoners*, 13 J. STRATEGIC SEC., no. 1, 2020, at 82, 98.

171. *Id.*

172. *Id.*

as a Muslim to help the Syrian people."[173] In one study of ISIS's recruitment practices, researchers noted that 24.7% of foreign recruits said that YouTube specifically influenced their decision to join ISIS.[174] Additionally, ISIS has recorded acts of violence such as beheadings.[175] It then incorporated these recordings into recruitment videos and disseminated the content across social media, which aided the group as it grew over 40,000 foreign members.[176] Initial online radicalization efforts are then bolstered by in-person reinforcement; importantly, the inverse can also be true.[177]

In addition to recruitment, ISIS also benefits from ICSs as a strategic tool. For example, in 2015, an essay written by a purported ISIS supporter in Libya was widely circulated online to gain support for ISIS's expansion in the country by fomenting divisions between rival governmental and parliamentary factions.[178] Indeed, some commenters have noted that creating an online propaganda machine was just as integral to ISIS's strategy throughout Libya as any of its tangible, tactical efforts in the region.[179] ISIS has also used social media to livestream large-scale violence, raise funds for arms and munitions, and promote its identity as a potent militant force.[180] Despite the critical role social media played in ISIS's growth and acts of terror, Section 230 has shielded ICSs from liability for both facilitating terrorist connections and hosting terrorists' content and, therefore, from facing any meaningful form of accountability.

B. Facebook's Counterterrorism Efforts

Facebook is fully aware that terrorism proliferates on its platform. And while it has taken steps to mitigate the spread of terrorist accounts and propaganda, some commentators suggest it has not gone far enough. Facebook employs a robust content moderation strategy, i.e., the process by

173. *Id.*

174. *See id.* at 101 (featuring a table with more in-depth information about foreign recruits and the influences that pushed them to join ISIS).

175. Matthew E. Schwartz & Hannah Allam, *ISIS Claims Responsibility for Easter Sunday Bombings in Sri Lanka*, NPR (Apr. 23, 2019, 5:59 AM), https://www.npr.org/2019/04/23/716266428/sri-lankan-official-says-bombings-are-retaliation-for-new-zealand-massacre [https://perma.cc/JN26-CF53] (noting that ISIS released photos and a video supposedly "show[ing] eight attackers" pledging allegiance to the group's leader in the aftermath of the Sri Lanka Easter Sunday bombings in 2019).

176. *See* Speckhard, *supra* note 170, at 16 (reporting that ISIS has recruited 40,000 foreign fighters using videos posted on social media).

177. *ISIS Online Hearing*, *supra* note 12, at 2.

178. *How the Islamic State Rose*, *supra* note 160, at 11.

179. *See, e.g.*, *id.* at 16 (explaining that ISIS's propaganda machine helped it recruit new members to strengthen its militia and to create disorder in rival governments).

180. *See id.* at 21 n.85 ("Abu Hafs al-Djazairi and Abu al-Bara al-Djazairi, two Algerian ISIS recruits, vowed to wage a 'long war' in Algeria on their way to Andalusia [on Facebook].").

which Facebook takes down content that violates site policies.[181] Through this moderation, Facebook attempts to detect terrorists' content through centralized and hybrid approaches, which incorporate both algorithmic and human review.[182] Facebook's algorithms are written to detect visual and textual indications that a particular account or piece of content is terrorism related.[183] The algorithms also use language-matching tools that seek to learn from language patterns over time.[184] Sometimes, Facebook's algorithms send content that is not clearly in violation of the platform's policies to the human moderators for review.[185] Additionally, Facebook's users can manually report content that algorithms fail to detect, which is then reviewed by human content moderators.[186]

However, this internal review is rife with imperfection. Consider that Facebook has over 2.8 billion active monthly users.[187] While algorithms and content moderators attempt to effectively monitor speech, the process is complicated by linguistic, contextual, and cultural nuance. Not to mention that these complications are particular to each of the 111 languages in which Facebook offers its services.[188] When factoring in the potential rate of human error, it becomes clear that content moderation is a difficult task. For example, Facebook indicated that it failed to remove terrorist content in the aftermath of the Sri Lankan attacks because its algorithms could not process Sinhala, the primary language spoken in Sri Lanka, and Facebook did not employ enough content moderators who spoke it.[189] Facebook reports the effectiveness of its content moderation practices in its Community Standards

181. Spandana Singh, *Everything in Moderation*, NEW AM. 22 (July 15, 2019, 10:21 AM), https://d1y8sb8igg2f8e.cloudfront.net/documents/Everything_in_Moderation_2019-07-15_142127_tq36vr4.pdf [https://perma.cc/7LGK-BR9Z].

182. *Id.* Facebook employs 30,000 people with a platform-security focus, including content moderators. *Id.*

183. *Id.*

184. *Id.*

185. *Id.* at 23.

186. *Id.* at 24.

187. *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2021*, STATISTA (Aug. 2, 2021), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [https://perma.cc/7XG2-6QST].

188. Maggie Fick & Paresh Dave, *Facebook's Flood of Languages Leave It Struggling to Monitor Content*, REUTERS (Apr. 23, 2019, 2:01 AM), https://www.reuters.com/article/us-facebook-languages-insight-idUSKCN1RZ0DW [https://perma.cc/KG6N-FK5W].

189. *See* Newley Purnell, *Sri Lankan Islamist Called for Violence on Facebook Before Easter Attacks*, WALL ST. J. (Apr. 30, 2019, 3:17 PM), https://www.wsj.com/articles/sri-lankan-islamist-called-for-violence-on-facebook-before-easter-attacks-11556650954 [https://perma.cc/87KK-WMQ8] (reporting that Facebook acknowledged it had limited capacity to review content in Sinhalaese); *see also* Max Fisher, *Sri Lanka Blocks Social Media, Fearing More Violence*, N.Y. TIMES (Apr. 21, 2019), https://www.nytimes.com/2019/04/21/world/asia/sri-lanka-social-media.html [https://perma.cc/M32S-LEYN] (reporting on the Sri Lankan government's shutdown of social media after the attacks); Fick, *supra* note 188 (reporting that Facebook has named Sinhala as a priority for content moderation).

Enforcement Report. Its November 2019 Report touts that Facebook's algorithms detected 98.5% of terrorist content before it was reported.[190]

But note, all of these efforts center on *content*, not connectivity. Although a content-based approach to curtailing terrorism undoubtedly inhibits the number of connections terrorist organizations might make with potential recruits, it does not address Judge Katzmann's fundamental insight. That is, none of Facebook's efforts indicate that the company has considered reworking its algorithms to limit the frequency with which it suggests terrorist content, pages, and accounts to individuals who are susceptible to radicalization. Nor does it indicate that Facebook has engaged in meaningful efforts to limit incoming messages to individuals who interact with known or suspected terrorist content, which would undercut practices like love bombing.

Additionally, some sources speculate the Community Standards Enforcement Report is somewhat misleading. In a 2020 study, for example, the Institute for Strategic Dialogue tracked 288 Facebook accounts linked to a particular ISIS network over three months.[191] The ISIS-related group running the accounts "was able to exploit gaps in both" of Facebook's moderation systems "to generate tens of thousands of views" for its content.[192] The study also detected networks of ISIS supporters "plotting, preparing and launching [target] 'raids' on [particular] Facebook pages, including those belonging to the U.S. military and political leaders."[193] Indeed, researchers watched in real time as the ISIS-related group posted instructions for its followers to flood the comment sections of targeted accounts with terrorist material.[194] None of this was reflected in Facebook's Community Standards Enforcement Report.

The study suggested that ISIS successfully thwarted Facebook's algorithmic-moderation attempts because it is not particularly difficult to get around them.[195] ISIS uses low-tech strategies to avoid detection: sometimes it blurs its logo, breaks up text to avoid keyword detection, adds Facebook's video effects, or adds the branding of mainstream logos to its videos (Facebook attempted to create an algorithm that prevented the removal of mainstream news media reporting on ISIS).[196] After ISIS engaged in one

190. Guy Rosen, *Community Standards Enforcement Report, November 2019 Edition*, FACEBOOK (Nov. 13, 2019), https://about.fb.com/news/2019/11/community-standards-enforcement-report-nov-2019/ [https://perma.cc/TG5E-BEY4].

191. Gordon Corera, *ISIS 'Still Evading Detection on Facebook,' Report Says*, BBC NEWS (July 13, 2020), https://www.bbc.com/news/technology-53389657 [https://perma.cc/87WX-JVBR].

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

particularly large effort to create new accounts, it took Facebook three months to scrub all of the new profiles.[197]

In 2019, after the horrific Christchurch, New Zealand attacks were broadcast across social media in real time,[198] Facebook, Twitter, Microsoft, and YouTube, along with "experts in government, civil society and academia,"[199] created the Global Internet Forum to Counter Terrorism (GIFCT).[200] Its stated mission is to "prevent terrorists and violent extremists from exploiting digital platforms."[201] It is currently headed by a former Director of the National Counterterrorism Center,[202] staffed by five intelligence experts,[203] and governed by an external oversight board.[204]

IV. Legislative Efforts

Nevertheless, the federal government, not Mark Zuckerberg, is constitutionally mandated to advance national security interests.[205] At present, Section 230 creates immunity for ICSs rather than creating incentives for proactivity. Irrespective of private corporations' efforts, the federal government must play an active role in combatting terrorism online by developing standards for content-moderation practices and, as discussed in more detail below, developing mechanisms to hold ICSs responsible when they fail to meet those standards. Fortunately, of the dozens of proposals aimed at reforming Section 230, at least one seeks to compel precisely that result.

Some proposals seek to repeal Section 230 wholesale and replace it with nothing,[206] and others would add caveats to Section 230's "Good Samaritan"

197. *Id.*

198. Smith, *supra* note 169.

199. Monika Bickert & Erin Saltman, *An Update on Our Efforts to Combat Terrorism Online*, FACEBOOK (Dec. 20, 2019), https://about.fb.com/news/2019/12/counterterrorism-efforts-update/ [https://perma.cc/77LP-NT82].

200. *About*, GIFCT, https://gifct.org/about/ [https://perma.cc/U4G6-Q9MV].

201. *Id.*

202. *Nicholas Rasmussen*, GIFCT, https://gifct.org/?team=nicholas-rasmussen [https://perma.cc/NSN7-CUAR].

203. *Johannah Lowin*, GIFCT, https://gifct.org/?team=johannah-lowin [https://perma.cc/52T5-B7VF]; *Sarah Kenny*, GIFCT, https://gifct.org/?team=sarah-kenny [https://perma.cc/YAS7-FPP8]; *Dr. Erin Saltman*, GIFCT, https://gifct.org/?team=dr-erin-saltman-2 [https://perma.cc/NP7D-NG25]; *Tom Thorley*, GIFCT, https://gifct.org/?team=tom-thorley [https://perma.cc/HU87-AD7P]; *Dr. Nayanka Paquete Perdigão*, GIFCT, https://gifct.org/?team=dr-nayanka-perdigao [https://perma.cc/79V2-H4JS].

204. *Governance*, GIFCT, https://gifct.org/governance/ [https://perma.cc/6V4E-ZZTX].

205. U.S. CONST. art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion.").

206. *See, e.g.*, Abandoning Online Censorship Act, H.R. 8896, 116th Cong. (2020) (authored by Representative Louie Gohmert (R-TX)); A Bill to Repeal Section 230 of the Communications Act of 1934, S. 5020, 116th Cong. (2020) (authored by Senator Lindsey Graham (R-SC)).

provision, which is beyond the scope of this paper.[207] However, the following section will evaluate the underlying frameworks of two remaining categories of legislation: those imposing new obligations[208] and those that seek to limit Section 230's scope by removing its liability bar in some contexts.[209] While the Justice Department[210] and bipartisan proposals advocate for the latter approach,[211] Facebook's Section 230 case law, ISIS's use of social media, and Facebook's counterterrorism efforts suggest the former would better address the threats posed by international terrorists' social media use.

A. Amendments That Limit Section 230's Scope

Proposals that seek to limit Section 230's scope are modeled after a recently enacted amendment to the law, which creates private causes of action against ICSs for violations of the federal sex trafficking statute (FOSTA-SESTA).[212] FOSTA-SESTA states, in relevant part:

> An individual who is a victim of a violation of this chapter may bring a civil action against the perpetrator (or whoever knowingly benefits, financially or by receiving anything of value from participation in a venture which that person knew or should have known has engaged in an act in violation of this chapter) in an appropriate district court of

---

207. *See, e.g.*, Limiting Section 230 Immunity to Good Samaritans Act, S. 3983, 116th Cong. (2020) (authored by Senator Josh Hawley (R-MO)); Stopping Big Tech's Censorship Act, S. 4062, 116th Cong. (2020) (authored by former Senator Kelly Loeffler (R-GA)).

208. *See, e.g.*, Protect Speech Act, H.R. 8517, 116th Cong. (2020) (authored by Representative Jim Jordan (R-OH)); Platform Accountability and Consumer Transparency Act, S. 4066, 116th Cong. (2020) (authored by Senators Brian Schatz (D-HI) and John Thune (R-SD)); Stop Shielding Culpable Platforms Act, H.R. 2000, 116th Cong. (2021) (authored by Representative Jim Banks (R-IN)).

209. *See* Don't Push My Buttons Act, S. 4756, 116th Cong. (2020) (authored by Senator John Kennedy (R-LA) and Representative Paul Gosar (R-AZ)) (preventing companies from invoking Section 230 if they collect users' data); Protecting Americans from Dangerous Algorithms Act, H.R. 2154, 117th Cong. (2021) (authored by Tom Malinowski (D-NJ)) (creating an exception to Section 230 in claims arising from civil rights violations or international terrorism); Stop Suppressing Speech Act of 2020, S. 4828, 116th Cong. (2020) (authored by former Senator Kelly Loeffler (R-GA)) (creating an exception to Section 230 in claims arising from harassment, illegal content, or violence and terrorism); Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms (SAFE TECH Act) (2021) (authored by Senators Mark Warner (D-VA), Masie Hirono (D-HI), and Amy Klobuchar (D-MN)) (removing Section 230's protections for (1) claims arising from ads or other content ICSs are paid to make available, (2) when ICSs seek to bar injunctive relief arising from their failure to remove content that causes irreparable harm, and (3) civil rights violations, antitrust, stalking, human rights violations, and wrongful death).

210. *Section 230 — Nurturing Innovation or Fostering Unaccountability?*, DEP'T JUST. 14–20 (June 2020), https://www.justice.gov/file/1286331/download [https://perma.cc/SSD8-JAFM].

211. *See* Mark MacCarthy, *Back to the Future for Section 230 Reform*, BROOKINGS (Mar. 17, 2021), https://www.brookings.edu/blog/techtank/2021/03/17/back-to-the-future-for-section-230-reform/ [https://perma.cc/NTR9-C365] (reporting that a popular, bipartisan approach to Section 230 reform is creating carve-outs).

212. 47 U.S.C. § 230(e)(5).

> the United States and may recover damages and reasonable attorneys fees.[213]

Effectively, FOSTA-SESTA pierces Section 230's protections so that victims of sex trafficking can recover against ICSs when third parties are found to be posting ads for prostitution.[214] Congress amended Section 230 in 2018 out of recognition that it "was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[215] FOSTA-SESTA was enacted after a congressional investigation into Backpage.com concluded that the site knowingly facilitated criminal sex trafficking.[216] Before FOSTA-SESTA, some courts held that Section 230 prevented individuals from holding Backpage liable for its part in the sexual exploitation of sex trafficking victims.[217]

After the law passed, Craigslist closed its personal-ads section, Reddit updated its site policies to forbid exchanging sexual services for money, and the FBI shut down Backpage.com.[218] However, as of the time of writing, no individual has successfully recovered on a sex trafficking claim against an ICS since FOSTA-SESTA's enactment, and no government officials have brought suit.[219] Additionally, the law raised other serious problems. For example, a significant policy critique was that FOSTA-SESTA did not curtail sex work and trafficking.[220] Instead, the law's opponents say it pushed trafficking offline where sex workers and trafficking victims are more

213. 18 U.S.C. § 1595(a).

214. Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018, 1:08 PM), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom [https://perma.cc/EF6R-A5TZ].

215. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, § 2, 132 Stat. 1253, 1253 (2018).

216. Romano, *supra* note 214.

217. *E.g.*, Doe v. Backpage.com, LLC, 817 F.3d 12, 24 (1st Cir. 2016).

218. Romano, *supra* note 214. The Texas Supreme Court found that Facebook could be liable in a June 2021 decision. Brooke Sjoberg, *Texas Supreme Court Rules Facebook Can Be Held Liable for Sex Trafficking, citing SESTA/FOSTA*, DAILYDOT.COM (June 28, 2021, 2:03 PM), https://www.dailydot.com/debug/texas-supreme-court-ruling-sesta-fosta-section-230-facebook/ [https://perma.cc/MBM7-PDBL]. This Note was completed in May 2021.

219. *See* Mike Masnick, *Civil FOSTA Suits Start Showing Up in Court; Prove That FOSTA Supporters Were 100% Wrong About Who Would Be Targeted*, TECHDIRT (Jan. 9, 2020, 9:25 AM), https://www.techdirt.com/articles/20200103/22513743675/civil-fosta-suits-start-showing-up-court-prove-that-fosta-supporters-were-100-wrong-about-who-would-be-targeted.shtml [https://perma.cc/YMU9-W3NR] (describing lawsuits that have been filed but not yet resolved); *see also* Adi Robertson, *Reddit Faces Lawsuit for Failing to Remove Child Sexual Abuse Material*, VERGE (Apr. 25, 2021, 8:00 AM), https://www.theverge.com/2021/4/25/22399306/reddit-lawsuit-child-sexual-abuse-material-fosta-sesta-section-230 [https://perma.cc/R29E-V9QE] (noting results from the lawsuits are unclear and most cases filed under the law are ongoing).

220. Romano, *supra* note 214.

susceptible to exploitation and abuse.[221] Further, there is no evidence that trafficking rates have decreased overall, and it is possible that forcing trafficking offline (or to the dark web) has made it more difficult to track.[222]

There is little reason to believe that a similar liability carve-out in the international-terrorism context would be more effective. For example, none of the previously mentioned studies suggested that ISIS uses specialized platforms to communicate. Put simply, there does not appear to be an equivalent to Backpage.com in the international-terrorism context, at least not one that features prominently in scholarship or case law. Instead, observers and plaintiffs seem more concerned about terrorist activity on more general platforms like Facebook and Twitter. Thus, the only definitive "benefit" derived from FOSTA-SESTA, shutting down mainstream platforms' sex-work-oriented communities, is not likely to curtail terrorism or enable victims of terrorism to recover damages from ICSs.

Further, creating an exception for liability under the ATA probably will not assist plaintiffs in proving proximate causation, just as FOSTA-SESTA has not widely enabled plaintiffs to recover under federal sex trafficking laws because of the difficulty of establishing that ICSs acted with the requisite *mens rea*.[223] Additionally, FOSTA-SESTA has not resulted in greater federal involvement in civil sex trafficking cases.[224] Thus, there is little reason to believe a similar amendment would result in federal efforts to help victims of international terrorism. Indeed, subjecting ICSs to liability for terrorist content might disincentivize their current counterterrorism efforts, like GIFCT and the Transparency Report.

When FOSTA-SESTA was being debated, tech-friendly organizations told lawmakers, "If you sign this bill, every website will be affected . . . Free speech dies."[225] Of course, every website was not affected, free speech did not die, and several major ICSs took affirmative steps to limit trafficking on

221. *Id.*

222. Neetha Kurup, *Sex & Modern Slavery: Did the FOSTA-SESTA Acts Reduce Human Trafficking? Here's Why We Can't See Results*, MEAWW (July 22, 2020, 7:30 AM), https://meaww.com/sex-and-modern-slavery-trump-administration-fosta-sesta-human-trafficking-impact [https://perma.cc/N6EC-CKBZ]. Members of Congress have introduced a bill to commission a study to evaluate FOSTA-SESTA's impact. EJ Dickson, *How Sex Workers Helped Write a Bill to Study the Effects of SESTA/FOSTA*, ROLLING STONE (Dec. 4, 2019, 5:23 PM), https://www.rollingstone.com/culture/culture-features/sesta-fosta-sex-work-decriminalization-ro-khanna-921043/ [https://perma.cc/V3Z3-594Z].

223. *See* Masnick, *supra* note 219 (suggesting plaintiffs have been unable to satisfy *mens rea* element of federal sex trafficking laws, which requires an ICS's knowing participation).

224. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-385, SEX TRAFFICKING: ONLINE PLATFORMS AND FEDERAL PROSECUTIONS 25 (2021).

225. Danielle Citron & Quinta Jurecic, *FOSTA: The New Anti-Sex-Trafficking Legislation May Not End the Internet, But It's Not Good Law Either*, LAWFARE (Mar. 28, 2018, 2:41 PM), https://www.lawfareblog.com/fosta-new-anti-sex-trafficking-legislation-may-not-end-internet-its-not-good-law-either [https://perma.cc/KX5Q-4V8P].

their platforms. However, it is not clear that the amendment has had any meaningful impact on limiting sex trafficking; it has not enabled a significant number of sex trafficking victims to recover against ICSs, and it has not bolstered federal efforts to combat sex trafficking. Additionally, there is growing congressional skepticism surrounding FOSTA-SESTA's efficacy, so a similar amendment in the international-terrorism context might prove too contentious to pass.[226]

Most importantly, although the Supreme Court has not yet addressed whether Section 230 or FOSTA-SESTA are constitutional, there is reason to believe it will strike down both provisions in the near future. For example, the provisions surrounding Section 230 were struck down as improper abridgments of the First Amendment in 1997.[227] Further, Supreme Court Justice Clarence Thomas recently took the peculiar step of issuing a concurring opinion in a case declared moot by the Court. The opinion, *inter alia*, "fired a warning shot at social media giants" by suggesting they should be classified as common carriers.[228] Specifically, "[i]f the analogy between common carriers and digital platforms is correct, then an answer may arise for dissatisfied platform users."[229] That answer would likely result in Section 230 and surrounding amendments like FOSTA-SESTA being deemed unconstitutional abridgments of the First Amendment.[230] Thus, a FOSTA-SESTA-type amendment is an unattractive framework for grounding efforts to combat international terrorism online. Indeed, although the Supreme Court denied certiorari in several cases implicating Section 230 in 2020,[231] Court observers speculate it will reach the issue this term.

226. *See* Press Release, Ro Khanna, Representative, House of Representatives, Reps. Ro Khanna, Barbara Lee & Senators Elizabeth Warren, Ron Wyden Introduce Safe Sex Workers Study Act (Dec. 17, 2019), https://khanna.house.gov/media/press-releases/release-reps-ro-khanna-barbara-lee-senators-elizabeth-warren-ron-wyden [https://perma.cc/D95G-GH9L] (expressing concerns about the harms FOSTA-SESTA creates for sex workers).

227. Reno v. ACLU, 521 U.S. 844, 849 (1997). Note also that trial court held that the provisions violated the First and Fifth Amendments. ACLU v. Reno, 929 F. Supp. 824, 858 (E.D. Pa. 1996). In *Reno*, the Supreme Court noted "[r]egardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment." Reno, 521 U.S. at 870. Thus, because the Court left open the possibility of reaching the Fifth Amendment claims in another case, Section 230 is not on ironclad footing with respect to that Amendment either.

228. Marguerite Reardon, *A Supreme Court Justice Weighs In on Section 230: Here's What It Means*, CNET (Apr. 12, 2021, 9:57 AM), https://www.cnet.com/news/a-supreme-court-justice-weighs-in-on-section-230-heres-what-it-means/ [https://perma.cc/3E97-UMXQ].

229. Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1225 (2021).

230. Reardon, *supra* note 228.

231. Dyroff v. Ultimate Software Grp., Inc., 140 S. Ct. 2761 (2020); Force v. Facebook, Inc., 140 S. Ct. 2761 (2020).

B. Bank Secrecy Act: A Credible Alternative

Instead of a FOSTA-SESTA-type amendment, lawmakers might instead turn their attention to legislation modeled after the well-entrenched Bank Secrecy Act (BSA). Senators Joe Manchin and John Cornyn have proposed precisely this type of legislative alternative to Section 230, albeit one principally aimed at online opioid trafficking.[232]

The BSA was enacted during the Nixon Administration and was designed to address the mob's pervasive money laundering, but it also proved helpful to law enforcement in the 1980s during the War on Drugs.[233] In both the '70s and '80s, the BSA required banks to report transactions over $10,000 or any other suspicious activity.[234] Then, in 1990, Congress created the Financial Crimes Enforcement Network (FinCEN) to provide a central locus for detecting, investigating, and prosecuting money laundering and other financial crimes.[235] FinCEN also created "Suspicious Activities Reports," strengthened existing bank identity verification and record-keeping requirements, and required the federal government to adopt new national strategies to address money laundering.[236] In 2001, detecting terrorist financing became the principal objective of the BSA.[237] The USA PATRIOT Act mandated that banks conduct even more rigorous oversight in the international-terrorism context. For example, it adopted exacting "Customer Due Diligence" standards, which compelled banks to create watchlists and conduct intensive sanctions screenings in international transactions.[238]

Overall, the BSA imposes significant burdens, including large fines, on financial institutions to incentivize reporting related to "terrorist financing."[239] The same burdens could be imposed on ICSs to incentivize moderation of terrorist content. Indeed, aspects of the underlying transactions also indicate that the BSA model would be effective. For example, under the BSA banks are required to spend billions of dollars on transaction-monitoring systems that meet federally mandated standards.[240] These transaction-

232. See Something, Say Something Online Act of 2020, S. 4758, 116th Cong. (2020) (authored by Senators Joe Machin (D-WV) and John Cornyn (R-TX)).

233. Jackie Wheeler, *The Bank Secrecy Act Turns 50: Five Decades of Anti-Money Laundering in the US*, JUMIO (Oct. 26, 2020), https://www.jumio.com/bank-secrecy-act-turns-50/ [https://perma.cc/LNG9-LXRZ].

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.*

238. *Id.*

239. Joshua Fruth, *Anti-Money Laundering Controls Failing to Detect Terrorists, Cartels, and Sanctioned States*, REUTERS (Mar. 14, 2018, 8:15 AM), https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV [https://perma.cc/8K95-6VCR].

240. *Id.*

monitoring systems are directed at targeting suspicious activity such as rapid money movement between accounts.[241] Content-monitoring systems could be similarly subjected to federally mandated standards, and rapid monetary transactions are hard to detect, much like ephemeral content posted by terrorists.

Indeed, there are already BSA-like regulations in the ICS space, albeit without the effective enforcement mechanisms used to compel good behavior from the financial sector. For example, when a U.S. law enforcement agency identifies a bank account associated with a terrorist group, FinCEN compels the bank to provide additional information about the accounts.[242] Likewise, under existing law the CIA or FBI can identify a post or an account associated with a terrorist organization and compel the ICS to provide information about that account.[243]

However, if a BSA investigation indicates a bank failed to detect or investigate the suspicious accounts, the bank is subjected to increased regulatory scrutiny, fines, or remediation.[244] There is no process by which an agency can similarly fine an ICS for failing to remove or detect an international terrorist's account; such a system might incentivize more proactive attempts to combat terrorism on its platform.

Moreover, it seems imbalanced to subject some industries to federal accountability for providing terrorists with an outlet to conduct their affairs while shielding others that provide analogous (and arguably more substantive) assistance to terrorists. Additionally, there is an institutional-legitimacy dimension that supports subjecting ICSs to proactive regulatory requirements. That is, the federal government issues standards that banks must comply with to combat international terrorism, whereas Mark Zuckerberg and other tech CEO's promulgate ICSs' counterterrorism efforts.

Admittedly, increasing ICSs' content-moderation obligations might be characterized as unduly burdensome. In the aftermath of 9/11, however, the federal government imposed anti-terrorism regulations on ICSs and many other industries like airlines, libraries, and healthcare facilities.[245] Then, like now, the federal government was interested in entrenching private-sector cooperation to serve legitimate national security interests and thwart future terrorist attacks.

Further, the BSA model is roughly analogous to successful international models like Germany's NetzDG, which is the imperfect-but-burgeoning

241. *Id.*

242. *Id.*

243. *Surveillance Under the USA Patriot Act*, ACLU, https://www.aclu.org/other/surveillance-under-usapatriot-act#:~:text=The%20Patriot%20Act%20increases%20the,held%20by%20a%20third%20parties [https://perma.cc/P45K-CCR9].

244. Fruth, *supra* note 239.

245. *Surveillance Under the USA Patriot Act*, *supra* note 243.

model of global counterterrorism regulation.[246] Adopting a BSA-style regulatory regime would also provide proactive government involvement in counterterrorism efforts without implicating the burden-of-proof challenges that exist within our current litigation-only approach. And, perhaps most importantly, unlike Section 230 and FOSTA-SESTA, the BSA has withstood constitutional challenges for decades.[247] Thus, it appears to be an attractive framework in which to ground Section 230 reform.

V. Conclusion and Recommendations for Further Research

In conclusion, the problems posed by Section 230 and international terrorists' use of the internet are relatively novel and undoubtedly complex. Possible solutions are untested, and trial and error will be needed to reach a more effective system of internet regulation. As a first step, policy analysts and lawmakers should complete more comprehensive reviews of Section 230 case law and terrorists' use of the internet before amending, repealing, or replacing Section 230. Further, Congress might conduct studies about the efficacy of FOSTA-SESTA and the BSA and whether these systems are empirically useful for addressing harm. Legislative solutions are more likely to be effective if they are crafted with a holistic, accurate understanding of the problems they seek to address.

Congress might also create a commission to evaluate the extent to which the judiciary accurately conceptualizes novel, web-based technology. Throughout the historical development of American common law, technological change has given rise to legal change. However, Section 230 case law suggests the federal judiciary seems to lack the technical expertise

246. Bill Graham & Stephanie MacLellan, *Overview of the Challenges Posed by Internet Platforms: Who Should Address Them and How?*, *in* CTR. FOR INT'L GOVERNANCE INNOVATION, GOVERNANCE INNOVATION FOR A CONNECTED WORLD 7 (Eileen Donahoe & Fen Olser Hampson eds., 2018).

247. *See, e.g.*, Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 55–56 (1974) (finding the possibility of disclosure of the identities of a banking association's members under the BSA insufficient to constitute a violation of the members' First Amendment rights); United States v. Miller, 425 U.S. 435, 444 n.6 (1976) (finding the BSA did not violate the First Amendment because "[t]here was no blanket reporting requirement" but rather the government "exercised its powers through narrowly directed subpoenas . . . subject to the legal restraints attendant to such process"); United States v. Fitzgibbon, 576 F.2d 279, 285 (10th Cir. 1978) (first citing Cal. Bankers Ass'n v. Shultz, 425 U.S. 435 (1974); and then citing United States v. Miller, 425 U.S. 435 (1976)) (determining that the Supreme Court has rejected contentions that portions of the BSA violate the First and Fourth Amendments); United States v. Griffith, 515 F. Supp. 3d 106, 121 (S.D.N.Y. 2021) (citing United States v. Tannenbaum, 934 F.2d 8, 12 (2d Cir. 1991)) (quoting Screws v. United States, 325 U.S. 91 (1945) (plurality opinion)) (finding Bank Secrecy Act provision requiring reporting by financial institutions not void for vagueness when applied to an individual because the Act defined financial institutions to include "[a] person who engages as a business in dealing in or exchanging currency").

needed to evaluate causation in the context of web-based technology, especially when cases implicate algorithms. Overall, the federal government must enact practical reforms based on more complete information about how international terrorists and everyday Americans use technology. Section 230 reform provides an excellent place to start.