Journal of Civil Rights and Economic Development

Volume 36
Issue 1 *Volume 36, Summer 2022, Issue 1*

Article 7

Technology's War on Terror: The Need for Platform Accountability in the Wake of a National Security Crisis

Meagan Schantz

TECHNOLOGY'S WAR ON TERROR: THE NEED FOR PLATFORM ACCOUNTABILITY IN THE WAKE OF A NATIONAL SECURITY CRISIS

MEAGAN SCHANTZ*

"[T]errorism today moves at the speed of social media . . . ."[1]

INTRODUCTION

January 6, 2021.[2] A day that "will live forever in infamy."[3] That day marked the first breach of the United States Capitol Building since 1814—and the second breach ever in American history (the

* J.D. Candidate, St. John's University School of Law, 2022.

1 *The Capital Insurrection: Unexplained Delays and Unanswered Questions (Part II): Hearing Before the H. Comm. on Oversight and Reform*, 117th Cong. (2021) (statement of Christopher Wray, Director, FBI).

2 On January 6, 2021, thousands of people stormed the United States Capitol Building during Congress's Electoral College certification process. Marc Fisher et al., *The Four-Hour Insurrection: How a Trump Mob Halted American Democracy*, WASH. POST (Jan. 7, 2021), https://www.washingtonpost.com/graphics/2021/politics/trump-insurrection-capitol/. The insurrection began shortly after President Donald Trump's "Save America" rally, where the President told a crowd of supporters, "[w]e're going to walk down to the Capitol, and we're going to cheer on our brave senators[] [and] congressmen and women. You have to show strength, and you have to be strong." *Id.* Members of the crowd proceeded down Pennsylvania Avenue and surrounded the Capitol, eventually breaching police barricades and fighting their way into the Capitol Building through broken windows and doors. *Id.* The Capitol was put on lockdown. *Id.* After the Capitol had been unsecured for four hours, five people were killed and countless others were injured, and the Capitol building suffered massive destruction. *See id.*; Amy Sherman, *A Timeline of What Trump Said Before Jan. 6 Capitol Riot*, POLITIFACT (Jan. 11, 2021), https://www.politifact.com/ article/2021/jan/11 /timeline-what-trump-said-jan-6-capitol-riot/.

3 NBC News, *Schumer: Jan. 6, 2021 "Will Live Forever in Infamy,"* NBC N.Y. (Jan. 7, 2021, 1:13 AM), https://www.nbcnewyork.com/news/politics/schumer-jan-6-2021-will-live-forever-in-infamy/2816513/; 161 CONG. REC. S55 (daily ed. Jan. 6, 2022) (statement of Sen. Majority Leader Charles E. Schumer).

first was during the War of 1812).[4] Five people lost their lives that day[5] and many more were injured in an unprecedented attack on American democracy. Yet, social media records show that "there were no surprises" as to what insurrectionists did on that infamous day.[6]

The plan to "storm the Capitol" began on less-trafficked social media sites, the "darker or more-obscure corners of the internet," including 8kun (formerly 8chan), Parler, Gab, and Telegram.[7] Angered by allegations of voter fraud and a "stolen election," users organized an attack on the United States Capitol to prevent the congressional certification of the national election results.[8] Users discussed which streets to take to gain unfettered access to the Capitol and which tools to bring to break open the Capitol's doors.[9] Some users inquired as to how violent the siege should get, with individuals posting about burning the Capitol and one 8kun user advocating for "Patriots" to "kill cops, kill security guards, kill federal employees and agents, and demand a recount."[10]

Discussions of protest and uprising were not limited to those sites. Posts about storming the Capitol, although less violent and graphic, also extended to mainstream platforms such as Twitter, Facebook, YouTube, and Instagram.[11] In December, a digital flyer

4 *See* Nora McGreevy, *The History of Violent Attacks on the U.S. Capitol*, SMITHSONIAN MAG. (Jan. 8, 2021), https://www.smithsonianmag.com/smart-news/history-violent-attacks-capitol-180976704/.

5 Ben Collins & Brandy Zadrozny, *Extremists Made Little Secret of Ambitions to "Occupy" Capitol in Weeks Before Attack*, NBC NEWS (Jan. 8, 2021, 12:36 PM), https://www.nbcnews.com/tech/internet/extremists-made-little-secret-ambitions-occupy-capital-weeks-attack-n1253499.

6 *Id.* (explaining that the Washington, D.C. Attorney General, Karl A. Racine, believed that law enforcement was aware of the threat posed by extremists on January 6, 2021).

7 Alex Woodward, *"Storm the Capitol": Violence Organised on Social Media as Warnings of Far-Right Post-Election Went Unheard*, INDEPENDENT (Jan. 8, 2021), https://www.independent.co.uk/news/world/americas/us-politics/capitol-riot-was-openly-organized-on-mainstream-social-media-b1784703.html; *see* Danielle Abril, *Trump Supporters Flock to MeWe, Gab, and Rumble After Parler goes Offline*, FORTUNE (Jan. 11, 2021, 9:16 PM), https://fortune.com/2021/01/11/mewe-gab-rumble-growth-parler-trump-bans-social-media-violence/ (explaining that Parler has since gone offline).

8 The election results were certified, confirming Joseph R. Biden, Jr. as the forty-sixth President of the United States. Abril, *supra* note 7; Donald Trump (@realDonaldTrump), TWITTER (Nov. 27, 2020, 10:56 AM), https://www.thetrumparchive.com/. Since Twitter suspended Donald Trump's account, the original tweets are no longer available.

9 *See* Sheera Frenkel, *The Storming of Capitol Hill was Organized on Social Media*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html.

10 *See* Collins & Zadrozny, *supra* note 5.

11 *See* Woodward, *supra* note 7.

titled "Operation Occupy the Capitol" was circulated on Facebook and Instagram by various right-wing groups.[12] On the night before the Capitol breach, increased traffic was recorded to "insurrectionist hashtags" on social media, including "1776" and "Occupy."[13]

Approximately twenty minutes before President Trump's "Save America" Washington D.C. rally ended, where he advocated for a takeback of the "stolen election," the first barricades outside of the Capitol were breached.[14] Thousands of people followed over the next few hours.[15] Once inside the Capitol, insurrectionists posted Livestream footage and photographs on Reddit, Facebook, Twitter, and YouTube of a mob storming the halls, breaking into offices, and stealing classified documents and government property.[16] Threats continued on Gab as users in the Capitol posted about finding Vice President Pence after he refused to overturn the results of the election.[17] Social media erupted as the American public watched the unprecedented attack from home. Nearly four hours after the attack began, President Trump posted a one-minute video to his social media accounts.[18] He told his followers in a since-deleted post, "Go home with love & in peace. Remember this day forever!"[19]

---

12 Collins & Zadrozny, *supra* note 5 ("That call to arms is just one of many warning signs on extremist sites and mainstream social media platforms that extremist experts say were easy to spot but ultimately disregarded by law enforcement . . . .").

13 *See id.*

14 *See* Lauren Leatherby et al., *How a Presidential Rally Turned Into a Capitol Rampage,* N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/interactive/2021/01/12/us/capitol-mob-timeline.html. The impact of the security breach led to increased training of Capitol Police. *See* Edward Segal, *Capitol Police to Hold First Joint Training Exercise on Capitol Grounds Since Riots*, FORBES (June 5, 2021, 4:46 PM), https://www.forbes.com/sites/edwardsegal/2021/06/05/capitol-police-to-hold-first-joint-training-exercise-on-capitol-grounds-since-riots/?sh=29addad06ef6.

15 *See* Leatherby et al., *supra* note 14.

16 *See* Sara Morrison, *The Capitol Rioters Put Themselves All Over Social Media. Now They're Getting Arrested*, VOX (Jan. 19, 2021, 6:52 PM), https://www.vox.com/recode/22218963/capitol-photos-legal-charges-fbi-police-facebook-twitter.

17 *See* Frenkel, *supra* note 9.

18 *See* Tasos Katopodis, *Trump Tells Capitol Rioters to "Go Home" but Repeatedly Pushes False Claim that Election Was Stolen*, CNBC (Jan. 6, 2021), https://www.cnbc.com/2021/01/06/trump-tells-capitol-rioters-to-go-home-now-but-still-calls-the-election-stolen.html; Kat Lonsdorf et al., *A Timeline of How the Jan. 6 Attack Unfolded—Including Who Said What and When*, NPR (Jan. 5, 2022, 5:00 AM), https://www.npr.org/2022/01/05/1069977469/a-timeline-of-how-the-jan-6-attack-unfolded-including-who-said-what-and-when.

19 Donald Trump (@realDonaldTrump), TWITTER (Jan. 6, 2021, 6:01PM), https://www.thetrumparchive.com/. The original tweet is no longer available. *Supra* note 8.

In the aftermath, public figures posted on Twitter and other platforms condemning the violent attack.[20] The American public expressed conflicting perspectives across numerous platforms, with some social media users condemning the act as one of domestic terrorism and others hailing the pride and patriotism of the day.[21] Internet "sleuths" emerged on Twitter and Instagram, posting photos of the protestors and openly naming them to assist in the FBI's investigation.[22] News of the attack spread around the world, eliciting international social media content.[23] International terrorist organizations, including ISIS, released online statements "hailing" the success of the Capitol assault and emphasized how the domestic unrest "w[ould] pay off" for terrorist organizations.[24] On January 8, 2021, in the midst of the rebuilding, President Trump was suspended and later banned from both Twitter and Facebook.[25]

As exhibited on January 6, social media has facilitated global communication by enabling individuals to connect and share content almost instantly. While increased connection can be positive, this expansion of communication has also facilitated the

[20] *E.g.*, Meryl Kornfield, *What Happened at the Capitol was "Domestic Terrorism," Lawmakers and Experts Say*, WASH. POST (Jan. 7, 2021), https://www.washingtonpost.com/national-security/2021/01/07/domestic-terrorism-capitol-mob/; Boris Johnson (@BorisJohnson), TWITTER (Jan. 6, 2021, 4:06 PM), https://twitter.com/borisjohnson/status/1346926138057220103?s=12.

[21] *See* Kornfield, *supra* note 20 (stating that public officials have largely viewed the attack as domestic terrorism, in contrast with neo-Nazi and far-right extremist groups who have celebrated the attack and used the event as propaganda).

[22] *See* Morrison, *supra* note 16. Currently, over 440 suspects have been arrested in connection to the Capitol insurrection. Clare Hymes & Cassidy McDonald, *440 have been Arrested in the Capitol Riot Investigation but the FBI is Still Looking for Suspects Accused of Vicious Attacks on Officers*, CBS NEWS (May 7, 2021, 4:47 PM), https://www.cbsnews.com/news/capitol-riot-arrests-fbi-wanted-officer-assaults-daniel-hodges/.

[23] *See* Ghaith Alsayed, *Photograph of Syrian Graffiti Artist Aziz Al-Asmar Creating Image of Capitol Breach*, NBC NEWS (Jan. 9, 2021, 1:42 AM), https://www.nbcnews.com/politics/congress/live-blog/2021-01-08-capitol-riots-electoral-vote-count-n1253384/ncrd1253520#blogHeader.

[24] *See* Bridget Johnson, *ISIS Hails Capitol Riot, Says U.S. Unrest 'Will Pay Off' for Terror Group*, HOMELAND SEC. TODAY (Jan. 8, 2021), https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-hails-capitol-riot-says-u-s-unrest-will-pay-off-for-terror-group/.

[25] *See* Kate Conger & Mike Isaac, *Twitter Permanently Bans Trump, Capping Online Revolt*, N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html; Kevin Breuninger, *Trump Blog Page Shuts Down for Good*, CNBC (June 2, 2021, 10:03 AM), https://www.cnbc.com/2021/06/02/trump-blog-page-shuts-down-for-good.html (explaining Donald Trump recently attempted to create his own blogging site, "From the Desk of Donald J. Trump," but the site was permanently shut down in June 2021).

circulation of terrorist and extremist content.[26] For many users, terrorism is not a part of the daily social media experience. However, its absence in "mainstream" social media is not representative of the wider landscape. Between August 2015 and December 2017, Twitter suspended 1,210,357 accounts for promoting terrorist content.[27] From June to December 2017, YouTube removed approximately 150,000 videos for promoting extremist content.[28] In 2018, Facebook "took action" on 9.4 million posts associated with al-Qaeda and ISIS.[29]

The threat of both international and domestic terrorism is largely perpetuated by social media because social media is a platform for recruitment and communication. Although social media platforms already have regulatory methods to remove content deemed unfit under a website's community standards,[30] greater action is needed to prevent the spread of terrorism on social media. Accordingly, this note proposes that social media companies be held liable when social media plays a clear role in the planning, organizing, and execution of an attack.[31] The current law, specifically section 230 of the Communications Decency Act and the Anti-Terrorism Act, absolves social media companies of

26 *See* U.S. NAT'L SEC. COUNCIL, NATIONAL STRATEGY FOR COUNTERING DOMESTIC TERRORISM (2021) https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf. Social media allows users to connect around the world, expediting the spread of news and other content. *Id*. Alongside those benefits, however, is the frightening spread of terrorism. *See id*. Recently, President Biden recognized this threat in his plan to counter domestic terrorism, which includes increasing resources, strengthening the Domestic Terrorism Executive Committee, and working privately with social media companies. *See id.*

27 *See* Stuart Macdonald et al., *Regulating Terrorist Content on Social Media: Automation and the Rule of Law*, 15 INT'L J. OF L. IN CONTEXT (SPECIAL ISSUE) 2–3 (2019) (stating that Twitter improved its AI processes from 2013-2014 statistics, where algorithms seemingly connected at-risk users with extremist pages).

28 *See id.* at 3.

29 Monika Bickert & Brian Fishman, *Hard Questions: What Are We Doing to Stay Ahead of Terrorists?*, META (Nov. 8, 2018), https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/.

30 *See Community Standards*, FACEBOOK, https://m.facebook.com/community standards/ (last visited Jan. 22, 2022); FACEBOOK, *Content Standards Forum- December 11, 2018*, https://about.fb.com/wp-content/uploads/2018/11/12.11.18-Content-Standard-Forum-Minutes-.pdf (last visited Jan. 22, 2022) (stating that Facebook removes content that "expresses support or praise for [terrorist] groups, leaders, or individuals").

31 A specific standard of review is beyond the scope of this note. While playing a "*clear role* in planning, organizing, and execution" suggests a threshold of gross negligence, it is beyond the scope of this note to determine the exact standard as to how extreme the failure to act must be. For example, determining the minimum number of views on certain extremist content that would signal gross misconduct in failing to remove a post would likely not be feasible. Furthermore, if such standards were set, that would raise other issues regarding manpower, costs, enforcement, etc.

responsibility for terrorist attacks that start and develop on social media platforms.[32] This note argues that section 230 should be amended to reduce the broad immunity provided to social media platforms. This amendment would result in increased liability for social media companies in social media-related terrorism, thereby advancing the safety and security of society and promoting the legal rights of victims and their families by incentivizing social media platforms to take care that they do not enable the planning, organizing, or execution of terrorist attacks. Additionally, the Anti-Terrorism Act should be amended to provide legal recourse for domestic terrorist attacks to force social media companies to identify and remove posts that threaten domestic terrorism and provide an opportunity for victims and their families to bring legal action.

Part I of this note will address the presence of terrorism on social media. Part IA will provide a background of social media, showing that increased regulation of terrorist content is critical due to social media's widespread accessibility and popularity in society. Part IB will provide a comprehensive overview of how social media platforms address terrorism on their sites, including the content that social media companies look for and methods of mitigation and removal; this section will also address the threat of terrorism, specifically the existence of both international and domestic actors who post terrorist content, on social media. Part IC will explain the current regulations affecting social media content and terrorism within the United States. These regulations include section 230 of the Communications Decency Act and the Anti-Terrorism Act (ATA); the former focuses on the protections provided to social media platforms, whereas the Anti-Terrorism Act focuses on acts of terrorism.

Part II will propose that section 230 of the Communications Decency Act and the Anti-Terrorism Act be amended to hold social media companies accountable for the publication of terrorist

[32] *See* 47 U.S.C. § 230(c)(2) ("No provider or user of an interactive computer service shall be held liable on account of—any action voluntarily taken in good faith to restrict access or [availability] of material that . . . the user considers to be . . . excessively violent . . . ."); Crosby v. Twitter Inc., 921 F.3d 617, 628 (6th Cir. 2019) (holding that Twitter was not liable for the execution of the Pulse Nightclub attack); Fields v. Twitter Inc., 881 F.3d 739, 741 (9th Cir. 2018) (holding that Twitter was not liable for the murder of two United States government contractors in Jordan, despite the shooter's engagement with ISIS content on social media).

content on social media platforms. Section 230 of the Communications Decency Act should be amended by rolling back the broad immunity provided to network operators. By amending the scope of coverage that section 230 offers, social media companies will be more accountable for monitoring threats to national security. Furthermore, victims of terrorist attacks will have legal recourse against otherwise "off-limits" social media platforms.

However, Part II will also explain that a balance must be struck to ensure that liability is narrowly defined, so as not to place an undue burden on social media companies. Additionally, the Anti-Terrorism Act should be amended to allow recovery for both international and domestic terrorist attacks. Expanding the statute to include domestic terrorist attacks would place greater pressure on social media companies to identify and remove domestic terrorist content and would provide a broader scope of redress for victims and their families.

I. BACKGROUND

A. Social Media is a Staple of Modern Society

Social media networks enable users to connect in previously unimaginable ways. Due to its accessibility and convenience, social media has become a critical force in American society and around the world. Because of the large, powerful role social media plays in modern society, regulation must be implemented to ensure that social media companies take extra care to maintain a safe online environment.

Social media is defined as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as

videos)."[33] The growth of these networks began in the 1990s as online blogging became increasingly popular.[34] The first social platforms, including Friendster and MySpace, developed in the late 1990s and early 2000s.[35] While those sites enjoyed the majority of the social media market for several years, they were later replaced with sites like Facebook in 2004 and Twitter in 2006, which offered different user experiences and consequently pulled users away from the original platforms.[36] This trend of fluctuating platform popularity continues today, as sites such as Telegram and Gab continue to grow, threatening to do to Facebook and Twitter what those sites did to Friendster and MySpace in the early 2000s.

Social media is a staple of modern society: about 70% of adults use at least one platform.[37] According to a 2018 study conducted by the Pew Research Center, more than two-thirds of Americans get some form of news from social media sites.[38] Namely, 43% of Americans get their news from Facebook, 21% from YouTube, and 12% from Twitter.[39] Consumption of social media news, and people's preferences of platforms, are largely dependent on factors such as race, gender, age, and political affiliation.[40] For example, 26% of social media users aged 18-29 prefer to receive their news from Facebook, compared to 40% of social media users aged 30-49 who use Facebook as their primary news source.[41] More than half

---

33 *Social Media*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/social%20media (last visited Mar. 1, 2021). For the purposes of this note, the term "social media" will be confined to digital platforms, such as Facebook, YouTube, and Twitter.

34 *See* Matthew Jones, *The Complete History of Social Media: A Timeline of the Invention of Online Networking*, HIST. COOPERATIVE (June 16, 2015), https://historycooperative.org/the-history-of-social-media/. As accessibility to the Internet increased, users enjoyed the ability to write about their daily experiences and know that their friends and families could read them. *Id.*

35 *Id.*

36 *Id.* Twitter allowed users to post 140 characters per Tweet (now 280 characters) to their list of "followers." *Id.* Facebook, originally branded as a college website, allows users to post a variety of media to their "friends." *Id.*

37 Summer Allen, *Social Media's Growing Impact on Our Lives*, AMERICAN PSYCHOL. ASS'N (Sept. 20, 2019), https://www.apa.org/members/content/social-media-research ("Whereas only five percent of adults in the United States reported using a social media platform in 2005, that number is now around 70 percent.").

38 Elisa Shearer & Katerina Eva Matsa, *News Use Across Social Media Platforms 2018*, PEW RES. CTR. (Sept. 10, 2018), https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ ("About two-thirds of American adults (68%) say they at least occasionally get news on social media, about the same share as at this time in 2017 . . . .").

39 *See id.*

40 *See id.*

41 *See id.*

of Americans expect social media news to be "largely inaccurate"; nevertheless, most still rely on their social media platforms for news out of convenience.[42]

Because of their large role in our daily lives, social media platforms are consistently scrutinized.[43] Recently, there has been a greater call for platforms to act against harmful speech, such as hate speech and misinformation.[44] Campaigns like Stop the Hate for Profit have garnered attention from celebrities and large companies alike, advocating for social media platforms to adopt a tougher position on offensive content and language.[45] Indeed, as Facebook, Twitter, and YouTube have attempted to strengthen their campaigns against misinformation in the wake of the presidential election, sites like Telegram and Gab have attracted users on the allure of promoting "free speech."[46] Telegram and Gab are not as popular as the mainstream platforms, but the continued movement of users based on politics and ideology reflects the expansive landscape of social media. While the campaigns against hate speech and misinformation and calls for action are important steps in the right direction, more work needs to be done to combat the presence of terrorism on social media by making social media

---

[42] *See id.* ("A majority (57%) say they expect the news they see on social media to be largely inaccurate.").

[43] *See* Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ ("In addition to the concerns about privacy and social media platforms uncovered in our surveys, related research shows that just 5% of social media users trust the information that comes to them via the platforms 'a lot.'").

[44] *See* Barbara Ortutay & Tali Arbel, *Social Media Platforms Face a Reckoning Over Hate Speech*, AP NEWS (June 29, 2020), https://apnews.com/article/6d0b3359ee5379bd5624c9f1024a0eaf ("For years, social media platforms have fueled political polarization and hosted an explosion of hate speech. Now, with four months until the U.S. presidential election and the country's divisions reaching a boiling point, these companies are upping their game against bigotry and threats of violence.").

[45] *See* STOP HATE FOR PROFIT, https://www.stophateforprofit.org/ (last visited Oct. 18, 2020). Stop the Hate for Profit advocated for a boycott of Facebook until the platform claimed responsibility for hate speech posted on the site. *See Statement from Stop Hate for Profit on July 2020 Ad Pause Success and #StopHateforProfit Campaign*. Through ad boycotts from businesses and individual user boycotts, Stop the Hate sought to slow profits in exchange for a policy change towards "hate, bigotry, racism, antisemitism, and disinformation." *See #StopHateForProfit September 2020 Week of Action*. Although this note does not focus on hate speech, these campaigns show a greater public pressure to regulate harmful content.

[46] *See* Alex Newhouse, *Right-Wing Users Flock to Parler as Social Media Giants Rein in Misinformation*, PBS (Dec. 3, 2020, 1:27 PM), https://www.pbs.org/newshour/nation/right-wing-users-flock-to-parler-as-social-media-giants-rein-in-misinformation (explaining that Parler and other sites attracted members of the "polarized public," who are able to further conspiracy theories through this unregulated platform).

companies accountable for the harmful content posted on their platforms.

B. Social Media-based Terrorism is a Complex Issue that Requires Multifaceted Solutions

Terrorism on social media remains a significant threat to national security in the United States. Terrorist organizations utilize social media to recruit members, disseminate propaganda, and broadcast violence to instill fear in others.[47] Social media platforms have responded by implementing regulatory policies to mitigate the spread of extremism. However, these policies, alone, are insufficient.

i. Social Media is Used by Terrorist Organizations to Recruit, Disseminate Propaganda, and Broadcast Violence.

Social media is used as a tool to advance various terrorist organizations' interests through, for example, recruiting, communicating through the publication of propaganda, gathering intelligence, and instilling fear.[48] According to a study conducted by Gabriel Weimann of the University of Haifa, approximately 90% of "organized terrorism" takes place on social media.[49] This significant statistic is attributable to accessibility, cost, and the ability to disseminate widespread messages.[50] According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START),

> Nearly two-thirds of extremists used Facebook for radicalization or mobilization. . . . YouTube was the second most frequently used platform among

47 *See* WIKIPEDIA, INFORMATION, PEOPLE, AND TECHNOLOGY, at 192 (2005) (citing a terrorism on social media study).

48 *See id.*

49 *See id.*

50 *See id.*

> extremists, with a usage rate of nearly one third. The third most popular social media platform was Twitter, which was utilized by nearly a quarter of extremists . . . .[51]

A social media platform may serve as a source for direct communication between organizations, or an organization and an individual, for recruitment or radicalization.[52] According to Dr. Erin Marie Saltman, who managed Facebook's counterterrorism policies, the internet itself does not radicalize a vulnerable individual or population; it merely serves as a *catalyst* for extremism by providing "tools, scale, and rapidity that doesn't exist elsewhere."[53] This concept was particularly apparent during the COVID-19 pandemic, where disenfranchised teenagers expressed an interest in extremism in the wake of lockdowns, isolation, and more time spent on social media.[54]

Social media has played a critical recruitment role for organizations like ISIS.[55] According to Dr. Saltman, social media redefined the idea of a "cloaked, dark figure of a jihadist" attempting to lure vulnerable individuals in.[56] Instead, extremists took a more "human" approach to social media and posted about their wedding days, the births of their children, cooking, and gaming culture.[57] Such content facilitates recruitment, as communication about seemingly ordinary topics evades platforms' user policy enforcement mechanisms.[58] However, when the dialogue develops into an illegal conversation, many "recruiters"

---

51 Michael Jensen et al., *The Use of Social Media by United States Extremists*, START, https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf.

52 *See* WIKIPEDIA, *supra* note 47.

53 Erin Marie Saltman, *How Young People Join Violent Extremist Groups – and How to Stop Them*, TED (Sept. 2017), https://www.ted.com/speakers/erin_marie_saltman.

54 *See* Jamie Grierson, *Children Showing Interest in Extremism, Says Senior Officer*, THE GUARDIAN (Sept. 23, 2020, 10:27 AM), https://www.theguardian.com/uk-news/2020/sep/23/children-interested-in-extremism-covid-says-neil-basu-counter-terrorism-officer ("When you've been locked down, with social media having such an influence on every single one of us in our daily lives, and you're able to sit there and just take all that in on a permanent basis with no other form of distraction or protective factor around you . . . that is a concern.").

55 *See* Saltman, *supra* note 53.

56 *Id.*

57 *See id.*

58 *See id.* (explaining that content moderators would have no cause for concern, assuming that the moderator was not aware of previous records or extremist history, regarding two users discussing video games or cooking).

know to move the discussion to a less regulated social media platform.[59] Therefore, despite platform regulations, recruitment can progress rapidly and essentially depart from the regulated grid before it can be thoroughly investigated.

Social media may also be used as a platform to disseminate propaganda directly, a method first used by al-Qaeda and later accelerated by ISIS.[60] ISIS propaganda promotes five key themes: strong governance and authority, military power, true religion, a call to action (Jihad), and fighting the global oppression of Muslims (the Umma).[61] This propaganda can range from images depicting a sense of brotherhood and community[62] to violent, gruesome videos of executions and beheadings.[63] The latter category of distributed content is typically referred to as "propaganda of the deed" (POTD).[64] POTD refers to "an act of political violence with the objective of creating a media event capable of energi[z]ing populations to bring about state revolution or social transformation."[65] POTD is considered a form of terrorism, though not all terrorism constitutes POTD.[66] This violent imagery is used to further the themes of Jihad and the oppression of the Umma.[67] For example, by depicting a missile strike or bombing of a small, predominantly Muslim town, al-Qaeda (or the original publisher) furthers their theme of fighting Western nations' oppression and execution of Muslim

59 *See id.* (stating that when actual, illegal details of recruitment or crime are raised, perpetrators know to move the conversation off of regulated sites like Facebook).

60 *See* WIKIPEDIA, *supra* note 47.

61 *See The Redirect Method*, MOONSHOT, https://moonshotteam.com/redirect-method/ (last visited Mar. 1, 2021). The Redirect Method is a pilot experiment organized by communication advisory networks to explore the impact of terrorist recruitment methods online. *See id.* Through media initiatives, the Redirect Method collected data on social media terrorism and created its own content to combat the threat. *See id.*

62 *See* Saltman, *supra* note 53 (showing photographs depicting a group of Muslim women with the caption, "sisterhood").

63 *See* WIKIPEDIA, *supra* note 47; Marilyn W. Thompson, *ISIS Murdered Her Son. But She Wasn't Going to Let that be His Only Legacy*, WASH. POST (May 10, 2018), https://www.washingtonpost.com/lifestyle/magazine/isis-murdered-her-son-but-she-wasnt-going-to-let-that-be-his-only-legacy/2018/05/08/138b34e6-3ced-11e8-a7d1-e4efec6389f0_story.html (discussing American journalist Jim Foley, whose gruesome murder by ISIS was posted on YouTube).

64 NEVILLE BOLT, THE VIOLENT IMAGE 2 (2012).

65 *See id.*

66 *See id.*

67 *See id.* at 47.

individuals.[68] This media, though often taken out of context, has proven to be a successful recruitment tactic.[69]

Social media platforms may also be used for broadcasting violent acts and garnering post-act publicity as a way to instill fear. For example, in 2019, a group of neo-Nazi extremists entered two mosques in Christchurch, New Zealand, and murdered 49 worshippers.[70] The shooting was recorded on a GoPro helmet camera and was simultaneously live-streamed on Facebook and reposted on Twitter and YouTube.[71] Exposing users to a deadly attack as it is occurring fulfills terrorism's purpose of instilling fear, particularly in Western countries.[72] Although the video was removed, images of the shocking attack remained on social media via news coverage.[73] The impact of these posts cannot be understated. The Christchurch attack was cited in the unsigned manifesto believed to be associated with Patrick Crusius, the twenty-year-old gunman who murdered twenty people in an El Paso Walmart.[74]

The use of social media by terrorist organizations for such purposes has led platforms to explicitly identify prohibited content that violates their rules and standards. Using legal definitions and independent criteria, each platform reviews and removes content as it deems necessary.

---

68 *See id.* (explaining that emotional content, even that which is inaccurate, assists in the process of radicalization).

69 *See id.* at 47.

70 *See* Max Boot, *Why Social Media and Terrorism Make a Perfect Fit*, THE WASH. POST (Mar. 16, 2019), https://www.washingtonpost.com/opinions/2019/03/16/why-social-media-terrorism-make-perfect-fit/.

71 *See id.*

72 *See id.*

73 *See id.* This note is not advocating for the censorship of legitimate news coverage, because the public should be informed of attacks. However, posts that glorify such attacks should be removed.

74 Tim Arango et al., *Minutes Before El Paso Killing, Hate-Filled Manifesto Appears Online*, N.Y. TIMES (Aug. 3, 2019), https://www.nytimes.com/2019/08/03/us/patrick-crusius-el-paso-shooter-manifesto.html. On August 3, 2019, Patrick Crusius killed twenty people and injured at least twenty others after a mass shooting in a Walmart in El Paso, Texas. Before driving almost ten hours to Walmart, Crusius released an unsigned, "anti-immigrant" manifesto online. The manifesto praised the Christchurch shooting and condemned the "Hispanic invasion of Texas." *See id.*

ii. Social Media Platforms Set the Standards for Prohibited Content

Each social media platform has a set of rules and guidelines that regulate user behavior, including prohibitions on dangerous or violent individuals and organizations.[75] Content that violates these guidelines often results in a deletion, as well as possible account suspension.[76]

Facebook removes posts related to terrorism and restricts terrorists and terrorist organizations from obtaining Facebook accounts.[77] Facebook defines a terrorist as "any non-state actor" that,

> (1) Engages in, advocates, or lends substantial support to purposive and planned acts of violence;
>
> (2) Which causes or attempts to cause death, injury or serious harm to civilians, or any other person not taking direct part in the hostilities in a situation of armed conflict, and/or significant damage to property linked to death, serious injury or serious harm to civilians;
>
> (3) With the intent to coerce, intimidate and/or influence a civilian population, government, or international organization; and
>
> (4) In order to achieve a political, religious, or ideological aim.[78]

Accordingly, any posts that display an act of terrorism, a symbol of a terrorist organization, or praise for an organization or act of

---

[75] For the purposes of this section, I will focus on primarily Facebook and Twitter's guidelines. *See Dangerous Individuals and Organizations*, META, https://www.facebook.com/communitystandards/dangerous_individuals_organizations (last visited Jan. 5, 2021) (providing the "Community Standards" of Facebook); *Violent Organizations Policy*, TWITTER, https://help.twitter.com/en/rules-and-policies/violent-groups (last visited Jan. 5, 2021) (providing the community guidelines of Twitter).

[76] *See* DANGEROUS INDIVIDUALS AND ORGANIZATIONS, *supra* note 74; VIOLENT ORGANIZATIONS POLICY, *supra* note 75.

[77] Facebook initially focused on accounts and content relating to ISIS and al-Qaeda, which resulted in the removal of twenty-six million posts. *See Dangerous Individuals And Organizations*, *supra* note 75; *Combating Hate And Extremism*, META (Sept. 17, 2019), https://about.fb.com/news/2019/09/combating-hate-and-extremism/.

[78] *See* DANGEROUS INDIVIDUALS AND ORGANIZATIONS, *supra* note 74.

terrorism is removed.[79] Facebook has commented that those standards are likely to change and that an updated definition would emphasize that a post must "attempt violence, particularly when directed toward civilians with the intent to coerce and intimidate . . . ." to violate its policy.[80] By expanding the definition and incorporating violence as a standard for removal, Facebook's rule seemingly bridges the gap between preventing censorship of vague, potentially harmless content and removing terrorist content.

Twitter relies on "national and international terrorism designations," as well as its own set of criteria, to determine what constitutes terrorist content.[81] Twitter defines "violent extremist groups," which include terrorist organizations, as groups who,

> (1) Identify through their stated purpose, publications, or actions as an extremist group;
>
> (2) Have engaged in, or currently engage in, violence and/or the promotion of violence as a means to further their cause; and
>
> (3) Target civilians in their acts and/or promotion of violence.[82]

Like Facebook, Twitter explains that violations of this policy include using a terrorist organization's symbol, recruiting for the organization, participating in violent acts on behalf of the organization, and providing services for the organization.[83] Such violations result in the removal of harmful content and account suspension.[84] Based on these guidelines, social media platforms utilize regulatory policies to monitor, and subsequently remove, content that violates platform standards.

79 *See id.*
80 *See* COMBATING HATE AND EXTREMISM, *supra* note 77.
81 *See* VIOLENT ORGANIZATIONS POLICY, *supra* note 75.
82 *See id.*
83 *See id.*
84 *See id.*

iii. Social Media Platforms Utilize Regulatory Methods to Remove Terrorist Content

To determine if the content meets a site's prohibited standards, social media platforms have responded by implementing their own regulatory methods, and these methods include the use of human intelligence and Artificial Intelligence (AI) which identify harmful content through algorithms and digital patterns.[85]

1. Artificial Intelligence as a Method of Content Regulation

AI regulation uses algorithms and digital identifiers, known as hashes, which regulate content through digital codes and patterns.[86] According to Facebook's Head of Global Policy Management, Monika Bickert,[87] terrorist propaganda is easily recognized by machines and algorithms due to common patterns and phrases.[88] Such content will often be caught before publication and will be blocked from dissemination.[89]

In 2016, social media companies began collaboratively working to record and share common patterns and phrases through the Global Internet Forum to Counter Terrorism (GIFCT).[90] This pact, in which Facebook, Microsoft, Twitter, and YouTube are all members, grants organizations access to a "shared industry hash database" that allows members to share "digital fingerprints for

85 *See* Bickert & Fishman, *supra* note 29 (stating that Facebook has enacted "machine learning" in conjunction with human review).

86 *See id.*

87 This paragraph will primarily focus on Facebook's counterterrorism policies because Facebook is the most transparent platform in terms of its pre-existing policies and new developments. *See id.*

88 Clea Simon, *The View from Inside Facebook*, HARV. GAZETTE (Dec. 5, 2018), https://news.harvard.edu/gazette/story/2018/12/facebook-leader-sits-down-with-harvards-jonathan-zittrain/. Facebook utilizes "Natural Language Understanding," which is an AI process that interprets content into more manageable patterns and categories of human speech. *See Natural Language Understanding At Facebook*, META, (Apr. 19, 2017), https://developers.facebook.com/videos/f8-2017/natural-language-understanding-facebook/.

89 *See* Simon, *supra* note 88. This type of regulation is often referred to as non-normative regulation. *See* Macdonald et al., *supra* note 28, at 184.

90 *See* Macdonald et al., *supra* note 27 at 184; *Update on the Global Internet Forum to Counter Terrorism*, TWITTER PUB. POL'Y (Dec. 4, 2017), https://blog.twitter.com/en_us/topics/events/2017/GIFCTupdate.html.

terrorist content" that can be utilized to recognize common elements of extremism.[91] Currently, the GIFCT database contains 200,000 digital hashes that allow member organizations to "identify and remove matching content that violates . . . [respective] policies – and sometimes block such [terrorist] content before it is even posted."[92]

Such technological safeguards are critical, but they are not infallible. For example, algorithms cannot always pick up on the "subtleties of expression," such as sarcasm or tone.[93] Furthermore, the permissibility of language is heavily context-dependent.[94] For instance, the Facebook Oversight Board issued its first five opinions in 2021, one of which involved the removal of a quote incorrectly attributed to Joseph Goebbels, the Reich Minister of Propaganda of Nazi Germany.[95] The Oversight Board overturned Facebook's decision to remove the quote, recognizing that although Goebbels is on Facebook's "Dangerous Individuals and Organizations" list, the post was not praising or glorifying him.[96] Such cases reflect the shortcomings of AI, namely the mistakes that can occur through flagging non-extremist material or conversely, failing to detect harmful threats. For these reasons, human-operated regulations are required to ensure that terrorist content does not go undetected.

---

91 *Update on the Global Internet Forum to Counter Terrorism*, TWITTER PUB. POL'Y (Dec. 4, 2017), https://blog.twitter.com/en_us/topics/events/2017/GIFCTupdate.html.

92 Macdonald et al., *supra* note 27, at 184.

93 To illustrate, posting "I'm going to kill you" may be interpreted as a threat by an AI program, even when it was intended to be a joke. *See* Simon, *supra* note 88; Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1054–55 (2017).

94 *See* Simon, *supra* note 88 (explaining how Facebook analyzes hate speech through a tiered system, where questionable phrases or terms that have not been defined are referred to one or more of the company's various content reviewers).

95 *Oversight Board Overturns Facebook Decision: Case 2020-005-FB-UA*, FACEBOOK OVERSIGHT BD. (Jan. 2021), https://oversightboard.com/news/141077647749726-oversight-board-overturns-facebook-decision-case-2020-005-fb-ua/. In October 2020, a user posted a quote "incorrectly attributed to Joseph Goebbels" in reference to President Trump. *Id.* The quote did not show photos of Goebbels, nor were there any references to Nazi symbols. *Id.* Nevertheless, the quote was removed for violating the "Dangerous Individuals and Organizations" Community Standard. *Id.*

96 *See id.* (noting that the removal of the post, which did not support the Nazi regime, should not have been removed pursuant to the unclear Dangerous Individuals and Organizations criteria).

2. Human Intelligence as an Additional Method of Content Regulation

In addition to technological safeguards, social media platforms have human-operated regulatory methods that monitor and remove terrorist content. On the ground level, social media users are expected to report content that violates the platform's standards, such as posts "celebrat[ing] or glorify[ing] violence."[97] This regulatory method, a normative method, is founded on the idea that users will self-police their social media community and bring attention to content that is not "fun and enjoyable for everyone."[98] According to YouTube and Twitter's community values, this appears to be the primary manner of reporting terrorist content.[99]

On a more organized level, suspected and convicted terrorists and their networks are tracked and removed from social media sites with help from news sources, government agencies, and activists.[100] For example, Facebook implemented a "fanning-out" process in which multilingual teams examine the pages liked, or events attended, by terrorists and their associated groups.[101] Through both Community Operations teams[102] and more than 150 "terrorism and safety specialists," Facebook scrutinizes posts and previous history to draw connections between suspect pages and

---

97 Natalie Andrews & Deepa Seetharaman, *Facebook Steps up Efforts Against Terrorism*, WALL ST. J. (Feb. 11, 2016, 7:39 PM), https://www.wsj.com/articles/facebook-steps-up-efforts-against-terrorism-1455237595 (stating that violent images or posts supporting an act of terrorism should be reported by independent users).

98 Social media sites operate with the expectation that users will flag or report disturbing content, such as images and videos depicting violence. These "human intelligence" methods work in conjunction with AI methods. *See* Macdonald et al., *supra* note 27, at 185.

99 *See Violent Criminal Organizations Policy*, GOOGLE: YOUTUBE HELP (last visited Jan. 1, 2021), https://support.google.com/youtube/answer/9229472?hl=en; *Addressing the Abuse of Tech to Spread Terrorist and Extremist Content*, TWITTER PUB. POL'Y (May 15, 2019), https://blog.twitter.com/en_us/topics/company/2019/addressing-the-abuse-of-tech-to-spread-terrorist-and-extremist-c.html (illustrating that self-reporting appears to be the primary method of regulation).

100 *See* Andrews & Seetharaman, *supra* note 97.

101 *Id.*

102 Community Operations addresses users' concerns on a variety of topics, including flagged content, internet connection, and reporting bugs or glitches in the system. *See Community Operations at Facebook*, META CAREERS (Sept. 27, 2016), https://www.facebook.com/careers/life/community-operations-at-facebook.

profiles.[103] In conjunction with that process, terrorists' profiles are also removed directly from the site.[104]

Like with AI-based regulation, human regulation has its shortcomings, however. With more than 70% of American adults using social media,[105] millions of posts are created and shared daily. Accordingly, it is not feasible for an individual to review and analyze every post to determine the level of the threat or if one exists at all.

3. Social Media Platforms Have Implemented Alternative Regulatory Approaches

In addition to using AI and "human intelligence" to analyze and report harmful content, social media platforms have implemented alternative methods of mitigating the spread and impact of terrorist content. One such form of combatting terrorist content on social media is called "counterspeech." According to the Dangerous Speech Project (DSP), counterspeech is a response intended to refute or undermine "hateful or dangerous speech online."[106] Counterspeech manifests itself in many different forms, including direct counterspeech (the counter speaker directly addresses the original speaker), as well as through the "contagion effect" (consistent exposure to positive counterspeech, which elicits the desire to also contribute counterspeech).[107]

---

103 *See* Monika Bickert & Brian Fishman, *Hard Questions: How We Counter Terrorism*, META (June 15, 2017), https://about.fb.com/news/2017/06/how-we-counter-terrorism/.

104 *See id.* There is debate as to how terrorist content should be treated. For example, removing and immediately deleting content may pose an investigative problem, specifically making it difficult for law enforcement to track a suspect and collect evidence for a subsequent trial. Conversely, simply censoring material or individuals frequently leads the content to appear elsewhere, under different profiles. *See Social Media Platforms Remove War Crimes Evidence*, HUMAN RIGHTS WATCH (Sept. 10, 2020, 1:00 AM), https://www.hrw.org/news/2020/09/10/social-media-platforms-remove-war-crimes-evidence#; Saltman, *supra* note 53.

105 *See* Allen, *supra* note 38.

106 The Dangerous Speech Project works to identify harmful speech on social media and mitigate its impact, without promoting or encouraging censorship. Cathy Buerger & Lucas Wright, *Counterspeech: A Literature Review*, DANGEROUS SPEECH PROJECT 1, 9 (Nov. 2019), https://dangerousspeech.org/wp-content/uploads/2019/11/Counterspeech-lit-review_complete-11.20.19-2.pdf.

107 *Id.* at 1–2.

Counterspeech tends to be a more public, albeit specialized, approach involving targeted responses towards certain content or a particular group. For example, in 2014, a German counterspeech organization amassed 100,000 counter-speakers to "like" and comment positive messages on various neo-Nazi Facebook pages.[108] Consequently, the hateful content was buried by messages of positivity and tolerance. Similarly, the Swedish Facebook group, Jagärhär ("I am here"), directs its members to post and like positive comments on specific news articles receiving hateful comments.[109] By increasing the traffic to positive comments, Facebook's algorithm places a greater emphasis on the counterspeech, deeming them "top comments" and consequently burying the negative speech.[110]

Counterspeech exists across many social media platforms, though some platforms have placed a greater emphasis on its use.[111] For example, Facebook adopted counterspeech as a platform tool to counter terrorist content.[112] Facebook's organized initiative offers different methods of engagement across multiple fields and disciplines.[113] According to Dr. Saltman, Facebook combines "large groups of civil society voices" with artists, poets, and comedians to produce counter-propaganda aimed at a specific demographic or region of the world.[114] For example, Facebook may strategically disseminate a satirical video "making fun of Islamophobia" to a targeted population of teenagers interested in white power music.[115] Views of that video would be subsequently tracked to measure engagement, in an attempt to detract

108 Deepa Seetharaman & Natalie Andrews, *Facebook Adds New Tool to Fight Terror: Counter Speech*, WALL ST. J. (Feb. 13, 2016, 1:42 PM), https://www.wsj.com/articles/BL-DGB-44855.

109 *Exploring Efforts to Reduce Online Hate at RightsCon 2019*, DANGEROUS SPEECH PROJECT (June 18, 2019), https://dangerousspeech.org/exploring-efforts-to-reduce-online-hate-at-rightscon-2019/.

110 *Id.*

111 *See* Binny Matthew et al., *Analyzing the Hate and Counter Speech Accounts on Twitter* (2018), https://arxiv.org/pdf/1812.02712.pdf; Seetharaman & Andrews, *supra* note 108 (noting that Facebook has recognized Counterspeech as a counterterrorism tool on their site, whereas platforms like Twitter have independent, "unaffiliated" counterspeech accounts).

112 *See* Seetharaman & Andrews, *supra* note 108.

113 *See Counterspeech*, FACEBOOK, https://counterspeech.fb.com/en/ (last visited Mar. 1, 2021).

114 Saltman, *supra* note 53.

115 *Id.*

viewership from terrorist content.[116] Similarly, the Redirect Method on YouTube counters extremist videos by offering conflicting advertisements, such as religious leaders denouncing extremism or ISIS defectors exposing the hypocrisy of the organization.[117]

In addition to the distribution of targeted material, platforms have started programs that directly engage with users suspected of showing an interest in extremism. For instance, Facebook began a "one-to-one" program.[118] Through this program, former members of terrorist and extremist organizations directly message Facebook users who show signs of interest in certain ideologies or organizations to discuss the realities of joining such organizations.[119] As of June 2016, 60% of users contacted through the program responded, and 60% of those who responded maintained engagement with their "one-to-one" contact.[120] According to Facebook's Chief Operating Officer, Sheryl Sandberg, counterspeech, perpetuated by former recruits to ISIS who left the organization and returned "to tell the truth," is "by far the best answer" to combat terrorist content.[121]

Despite the widespread implementation of counterspeech initiatives, their effectiveness is still debated. For example, a 2016 study conducted by Carla Schieb and Mike Preuss of the University of Münster concluded that counterspeech *could* effectively reach an original speaker, but the level of success depended on the "size of the group of hateful speakers."[122] Specifically, counterspeech activity produced greater success where the counter-speakers outnumbered the group of "hateful speakers."[123] Conversely, a 2018 study conducted by Jozef Miškolci regarding hate speech against the Roma in Slovakia

116 *See id.* (explaining how social media platforms measure the success of such initiatives).

117 *See* THE REDIRECT METHOD, https://moonshotteam.com/wp-content/uploads/2021/12/redirectmethod-fullmethod-PDF.pdf.

118 *See* Saltman, *supra* note 53.

119 *See id.* (noting that many former members try to dissuade engagement with organizations based on the façade of inclusion, which does not actually exist).

120 *Id.*

121 World Economic Forum, *The Transformation of Tomorrow*, YOUTUBE (Jan. 20, 2016), https://www.youtube.com/watch?v=mtXfzd53wRQ (explaining Facebook's program during a panel at the World Economic Forum Annual Meeting, which was meeting to discuss the future of technology).

122 Buerger & Wright, *supra* note 106, at 1.

123 *See id.*

found that direct counterspeech was ineffective in altering the original speaker's behavior but instead was effective in reaching a larger audience who could also engage in counterspeech.[124] Accordingly, the success of counterspeech is "[r]ight now an assumption [that] better ideas ultimately defeat worse ideas."[125]

Social media sites have implemented their regulatory methods through the use of AI and human expertise. While they have proven successful in identifying some terrorist posts,[126] there is still a need for improvement to stay ahead of such content. Terrorism remains a growing threat on social media, and in many cases, terrorist content remains unchecked.[127] Such situations where content is not removed, and a terrorist attack occurs as a result signal the need for stronger legal accountability.

iv. Identifying and Labeling Terrorism Remains a Challenge

Because terrorism is hard to define, it can be difficult to moderate on social media platforms. Before removing or regulating terrorist content, it must be identified, and where it is difficult to define, it is more difficult to regulate.[128]

1. Terrorism has Multiple Definitions

"There is no single, universally-accepted, definition of terrorism."[129] Therefore, while definitions may share common

124 *See id.* at 2.

125 *See* Seetharaman & Andrews, *supra* note 108.

126 *See* Bickert & Fishman, *supra* note 29 ("In Q2 2018, we took action on 9.4 million pieces of content related to ISIS, al-Qaeda, and their affiliates, the majority of which was old material surfaced using specialized techniques. In Q3 2018, overall takedowns of terrorist content declined to 3 million, of which 800,000 pieces of content were old, because our efforts to surface and remove old content on the platform in the second quarter had proven effective.").

127 *See* Frenkel, *supra* note 9.

128 *See* U.S. DEP'T OF JUST. FBI, TERRORISM 2002-2005, i, iv, https://www.fbi.gov/stats-services/publications/terrorism-2002-2005 (recognizing the different forms of terrorism and how the criteria do not easily define acts of terrorism).

129 *Id.*

elements, no two are truly identical.[130] This underscores a common theme of this note—the inconsistency of important legal definitions. The Code of Federal Regulations defines terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[131] Section 2331 of Title 18 of the United States Code provides two definitions of terrorism: one for international terrorism and a separate definition for domestic terrorism. The statute defines "international terrorism" as activities that,

> **(A)** involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
>
> **(B)** appear to be intended—
>
> **(i)** to intimidate or coerce a civilian population;
>
> **(ii)** to influence the policy of a government by intimidation or coercion; or
>
> **(iii)** to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> **(C)** occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by

130 *See* Wesley S. McCann & Nicholas Pimley, *Mixed Mandates: Issues Concerning Organizational and Statutory Definitions of Terrorism in the United States*, 32 TERRORISM & POL. VIOLENCE (2020), https://www.tandfonline.com/doi/full/10.1080/09546553.2017.1404457?scroll=top&needAccess=true ("Research has shown that developing a single definition of terrorism is not only unlikely[] but also quite difficult. Definitions of terrorism can arguably be influenced by cultural, social, and political factors."); Boaz Ganor, *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?*, 3 POLICE PRAC. & RES. (2002), https://www.tandfonline.com/doi/abs/10.1080/1561426022000032060 ("Most researchers tend to believe that an objective and internationally accepted definition of terrorism can never be agreed upon; after all, they say, 'one man's terrorist is another man's freedom fighter.'").

131 28 C.F.R. § 0.85(l) (1969).

> which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . .[132]

The statute defines "domestic terrorism" as activities that,

> **(A)** involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
>
> **(B)** appear to be intended—
>
> **(i)** to intimidate or coerce a civilian population;
>
> **(ii)** to influence the policy of a government by intimidation or coercion; or
>
> **(iii)** to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> **(C)** occur primarily within the territorial jurisdiction of the United States . . . .[133]

These two definitions provide a basis for recognizing both international and domestic terrorism. Accordingly, these definitions will guide further discussion on defining and identifying terrorism.

2. Designating Terrorist Organizations Provides a Starting Point for Identification

Designating terrorist organizations is critical to ensure continuous monitoring. In the social media context, the designation provides a foundation for platforms to easily identify and remove content. Namely, if an individual has ties to a particular designated organization, their profiles will be removed regardless of the content that they are posting.[134] Accordingly, the

---

132 18 U.S.C. § 2331(1).

133 § 2331(5).

134 *See generally* COMBATING HATE AND EXTREMISM, *supra* note 77 (stating Facebook's policy on content removal); DANGEROUS INDIVIDUALS AND ORGANIZATIONS, *supra* note 74.

designation process and implications are important for understanding how social media content is monitored.

Based on prior threats and attacks, the Department of Homeland Security (DHS) currently lists approximately seventy organizations as "designated foreign terrorist organizations."[135] These organizations include Hamas, Hizballah, al-Qaeda, al-Shabaab, Boko Haram, and ISIS.[136] Organizations are designated by the Bureau of Counterterrorism (CT) in the State Department, which examines the actual attacks executed by a foreign terrorist organization (FTO), evidence of any planned attacks, and whether the organization has the capability and true intent to execute any future attacks.[137] Once the CT determines that a group has met the statutory requirements of an FTO, a record is submitted to the Secretary of State, Attorney General, and Secretary of the Treasury for review.[138] Upon approval, the record is then transferred to Congress, which has seven days to block the designation.[139] If Congress fails to block the designation, a notice of designation is published in the Federal Register and the designation is implemented.[140]

The designation as a terrorist organization has legal implications for both members of an organization and unaffiliated individuals. For example, non-citizen members of designated FTOs are "inadmissible" into the United States.[141] As for unaffiliated persons, it is illegal to "knowingly provide 'material support or resources'" to designated FTOs, known as aiding and abetting the cause.[142] The latter reflects a common argument that

135 BUREAU OF DEMOCRACY, *Foreign Terrorist Organizations*, U.S. DEP'T OF ST., https://www.state.gov/foreign-terrorist-organizations/ (last visited Feb. 15, 2022).

136 *See id.*

137 *See id.* ("The Bureau of Counterterrorism in the State Department (CT) continually monitors the activities of terrorist groups active around the world to identify potential targets for designation.").

138 *See id.*

139 *See id.*

140 *See id.* ("Upon the expiration of the seven-day waiting period and in the absence of Congressional action to block the designation, notice of the designation is published in the Federal Register, at which point the designation takes effect.").

141 8 U.S.C. § 1182(a)(3)(B); *see, e.g.*, Luke Denne, *American-born ISIS Bride not a Citizen, Judge Rules*, NBC NEWS, (Nov. 15, 2019, 10:26 AM) https://www.nbcnews.com/news/world/american-born-isis-bride-not-citizen-judge-rules-n1082766 (stating that ISIS bride Hoda Muthana would not be allowed to enter the country after fleeing to Syria and marrying three ISIS fighters).

142 *See* U.S. Dep't of State, *supra* note 135 (quoting 18 U.S.C. § 2339A); 18 U.S.C. § 2339A (defining the term "material support or resources").

individuals make for holding social media companies liable for terrorist content: social media platforms are a resource for committing terrorist attacks by indirectly providing a platform for recruitment and communication.[143] This argument has been unsuccessful[144] and illustrates one of many failed attempts to hold social media platforms liable for the dissemination of terrorist content.

3. The Challenge and Hesitation in Labeling Domestic Terrorism

In addition to international terrorist threats, the United States is also subject to domestic terrorist threats. Despite a legal recognition of domestic terrorism in the United States, there is a lack of public information regarding domestic terrorism.[145] Currently, no law exists that focuses on regulating and preventing the threat of domestic terrorism, though Congress has made attempts at legislation in previous sessions.[146] Additionally, unlike the designation process of FTOs, there are currently no designated domestic terrorism organizations.[147] This makes it difficult to identify domestic threats, as there may not be "obvious" signs that an individual is working on behalf of a terrorist organization.[148] Experts calculate that domestic terrorism

143 *See generally*, Pennie v. Twitter, Inc., 281 F. Supp. 3d 874, 876–77 (N.D. Cal. 2017) (explaining that the Plaintiffs could not prove the direct connection between Hamas and the suspect, let alone between Twitter and the suspect).

144 *See id.* at 879–882 (referencing cases where this argument was similarly found unsuccessful).

145 *See* Kornfield, *supra* note 20 ("The FBI, which is investigating the violence, declined to comment when asked if the raid was considered domestic terrorism.").

146 *See, e.g.,* Domestic Terrorism Prevention Act of 2020, H.R. 5602, 116th Cong. (2nd Sess. 2020). H.R. 5602 advocated for greater access to information on domestic terrorism by DHS, DOJ, and FBI. Furthermore, the bill established a task force to examine all domestic threats, including white supremacy and neo-Nazism. The bill passed the House on September 21, 2020, but remained in committee in the Senate for the duration of the 116th Congress. *Id.*

147 *See Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the Comm. on Homeland Sec.*, 116th Cong. 43 (2019) (statement of Michael McGarrity, Assistant Director for the Counterterrorism Div., Fed. Bureau of Investigation, U.S. Dep't of Just.).

148 *See id.* (explaining that when terrorist groups are "actually designated" as such, it is easier to identify potential terrorists).

accounts for twenty percent of threats.[149] However, many of these threats appear to remain in a largely undefined "gray area."

DHS recognizes categories of domestic terrorism, characterized as Homegrown Violent Extremists (HVE) and Domestic Violent Extremists (DVE).[150] DHS defines an HVE as,

> [A] person of any citizenship who has lived . . . in the United States . . . [and] who is engaged in, or is preparing to engage in ideologically-motivated terrorist activities . . . in furtherance of political or social objectives promoted by a foreign terrorist organization (FTO), but is acting independently of direction by an FTO.[151]

DHS further notes that "HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor."[152] HVEs are largely referred to as "lone-wolf" terrorists.[153]

A DVE, though similar to an HVE, is defined as "[a]n individual based and operating primarily within the United States . . . without direction or inspiration from a foreign terrorist group . . . who seeks to further political or social goals . . . through unlawful acts of force or violence."[154] According to DHS, DVEs encompass White Supremacist Extremists (WSE), who are defined as "racially and ethnically motivated violent extremists."[155] DHS further narrows the definition, stating that "[t]he mere advocacy of

---

149 *See* Seth G. Jones et al., *The War Comes Home: The Evolution of Domestic Terrorism in the United States*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201021_Jones_War_Comes_Home_v2.pdf.

150 *See* U.S. DEP'T OF HOMELAND SEC., HOMELAND THREAT ASSESSMENT: OCTOBER 2020 17 (2020), https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf. The FBI also uses these definitions. FED. BUREAU OF INVESTIGATION, DOMESTIC TERRORISM: DEFINITIONS, TERMINOLOGY, AND METHODOLOGY 2 (2020), https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view.

151 *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 150, at 17 n.7.

152 *See id.*

153 *See* Mark Hamm, *Lone Wolf Terrorism in America*, U.S. DEP'T OF JUST.: OFF. OF JUST. PROGRAMS (Feb. 2013), https://www.ojp.gov/ncjrs/virtual-library/abstracts/lone-wolf-terrorism-america ("'Lone-wolf' terrorism is the term used to describe someone who acts alone in a terrorist attack without the help or encouragement of a government or a terrorist organization.").

154 *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 150, at 17 n.6.

155 *See id.* at 18.

political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute extremism, and may be constitutionally protected."[156] Hence, designating an individual as a DVE is highly context-dependent, which may result in hesitation to do so at all.

As noted in the DVE definition, an individual may post content considered to be offensive or to reference violence; however, that person still may not be deemed a DVE.[157] This caveat underscores the hesitation in identifying domestic terrorism: monitoring content that may pose a threat[158] must be balanced against an individual's right to post their opinions and invite conversation.[159] Additionally, domestic terrorism is often more difficult to identify logistically due to its overlap with international terrorism.[160] Accordingly, the challenge in defining domestic terrorist organizations makes it more difficult for platforms to remove terrorist speech based on group identification or association.

156 *See id.* at 17 n.6.

157 *See id.*

158 To prosecute a suspect for incitement of violence, including terrorism, the prosecution must show that the individual intended to incite or produce an unlawful action and the likelihood that the speech would incite imminent unlawful action. Brandenburg v. Ohio, 395 U.S. 444, 448–49 (1969). Accordingly, without knowing whether the user intends to execute an attack or intends violence from an otherwise vague post, a social media platform may leave the post up to avoid censorship. *See id.*; U.N. OFF. ON DRUGS AND CRIME, THE USE OF THE INTERNET FOR TERRORIST PURPOSES 39 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

159 Offensive language, or hate speech, is treated differently than terrorist content. For example, on Facebook, language that attacks a person or group of people based on a characteristic such as a nationality, ethnicity, gender, or sexual orientation is not permitted. Yet, discussion about excluding or segregating a certain group may be allowed in a political context. For example, posting "I don't want more immigrants" would be allowed to enable users to have a discussion about immigration. However, making a violent threat such as "[b]urn the immigrants" would be removed. *See* Simon, *supra* note 88; *Hate Speech*, META, https://transparency.fb.com/policies/community-standards/hate-speech/ (last visited Jan. 21, 2022) (explaining that Facebook does not allow hate speech, defined as "direct attack[s] against people . . . on the basis of . . . race, ethnicity, national origin, disability, religious affiliation, caste, sexual orientation, sex, gender identity and serious disease.").

160 This is particularly true for lone-wolf terrorism, where an individual may be a United States citizen, but becomes influenced or radicalized by international organizations. *See* Gregory D. Miller, *Blurred Lines: The New "Domestic" Terrorism*, 13 PERSP. ON TERRORISM 63 (June 2019) (stating that different elements are at play for recruiting and executing attacks, which may blur the lines between domestic and international terrorism).

C. Section 230 and the Anti-Terrorism Act Impact Decisions Regarding Social Media Terrorism

Section 230 of the Communications Decency Act and the Anti-Terrorism Act serve as two primary legal authorities regarding terrorism on social media. Section 230 provides immunity to network operators, absolving social media sites of liability for content published by third-party users.[161] The Anti-Terrorism Act, on the other hand, provides civil remedies for victims of international terrorist attacks.[162]

i. Section 230 Provides Broad Immunity to Network Operators

Section 230 of the Communications Decency Act serves as a primary guide in Internet liability cases and has elicited controversy and debate since its enactment on February 8, 1996.[163] The Communications Decency Act was originally proposed in 1995 by Senator James Exon (D-NE).[164] The bill's original purpose was to implement a punitive system for network operators who knowingly made "indecent material" available to minors.[165] The proposed bill was met with opposition, as individuals believed that it would lead to mass censorship (a

161 *See* 47 U.S.C. § 230(c)(1) ("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.").

162 *See* 18 U.S.C. § 2333(a) ("Any national of the United States injured . . . by reason of an act of international terrorism . . . may sue therefor in any appropriate district court of the United States and shall recover . . . damages . . . .").

163 Felix Gillette, *Section 230 Was Supposed to Make the Internet a Better Place. It Failed*, BLOOMBERG BUSINESSWEEK (Aug. 7, 2019, 4:00 AM), https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed (stating that conservatives tend to view section 230 as a tool for censorship, where liberals view section 230 as an "excuse" to ignore harmful content).

164 S. 314, 104th Cong. (1995).

165 *Id.* at § 4 ("Amends the Federal criminal code to: (1) increase the fine for broadcasting obscene, indecent, or profane language over the radio . . . .").

familiar argument today).[166] Yet despite the opposition, Senator Exon's proposal passed the Senate by a vote of 86-14.[167]

Concurrently, in 1995, the Supreme Court of New York decided *Stratton Oakmont v. Prodigy*.[168] Prodigy, a computer network operator, had published defamatory content about the plaintiff, Stratton Oakmont.[169] Stratton Oakmont sued, alleging that Prodigy was liable for the defamatory posts.[170] In its defense, Prodigy relied on *Cubby v. CompuServe*.[171] In *Cubby*, the network CompuServe published libelous content about Cubby, an electronic newsletter.[172] In that case, the Southern District of New York applied a standard that is protective of speakers, which in this case was network operator:

> A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to

166 *See* Gillette, *supra* note 163 ("Back in 1995, when the CDA was conceived, section 230 enjoyed bipartisan support from members of Congress, who believed that tech companies would do a better job at moderating the internet than federal regulators. But a growing number of hostile lawmakers are now criticizing Big Tech's safe harbor."). On May 28, 2020, President Donald Trump issued his "Executive Order on Preventing Online Censorship." Preventing Online Censorship, Exec. Order No. 13925, 85 FR 34079 (2020). This Executive Order accused Internet platforms like Twitter, Facebook, Instagram, and YouTube of "engaging in selective censorship that is harming our national discourse." *Id.* Specifically, the President claimed that networks flagged content that did not violate their standards, deleted accounts "with no warning, no rationale, and no recourse," and placed labels on posts reflecting political bias. *Id.* President Trump cited section 230 as a cause, stating that its scope should be narrowed. To redefine the scope of section 230, the President proposed enacting notice requirements, clarifying exceptions where a publisher could be held liable, and enacting a "good faith" measure when removing content. This is one example of how politics can influence the application of the law. *See id.*

167 *See* Gillette, *supra* note 163.

168 *See id.*; Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710, (N.Y. Sup. Ct. May 24, 1995).

169 *See Stratton Oakmont*, 1995 WL 323710, at *2 (stating that Prodigy was a publisher in large that "held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards," where the libelous statements were posted).

170 *Id.* at *1.

171 *Id.* at *3–4.

172 Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 137–38 (S.D.N.Y. 1991).

> CompuServe is whether it knew or had reason to know of the allegedly defamatory . . . statements.[173]

Accordingly, the court found that CompuServe was not liable for the defamatory posts.[174] Yet, in *Stratton Oakmont*, the court distinguished the two cases because, unlike CompuServe, Prodigy screened its content before publication.[175] Therefore, the court found Prodigy liable based upon the distinction between a distributor, like CompuServe, and a publisher, such as Prodigy, that reviewed its posts.[176]

This decision led to a call for greater protection of network operators because network operators could now be held liable for defamatory content on their sites that they were not even aware of.[177] Subsequently, Representative Ron Wyden (D-OR) and Representative Christopher Cox (R-CA) proposed the "Internet Freedom and Family Empowerment Act."[178] According to the bill, a computer service operator would not be treated as the publisher of any content posted on its site.[179] Additionally, under the bill's Good Samaritan provision, network operators would not be held liable for removing suspect content.[180] The "Internet Freedom and Family Empowerment Act" was combined with the Communications Decency Act and section 230 to make up Title V of the Telecommunications Act of 1996.[181] The package, including

---

173 *See id.* at 140–41.

174 *See id.* at 141. ("Because CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements, summary judgment in favor of CompuServe on the libel claim is granted.").

175 *See* Stratton Oakmont, 1995 WL 323710, at *4–5 ("The key distinction between CompuServe and *Prodigy* is [twofold.] First, *Prodigy* held itself out to the public and its members as controlling the content of its computer bulletin boards. Second, *Prodigy* implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce.").

176 *See id.* (finding that "*Prodigy* is a publisher rather than a distributor" because it used "technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste,'" which constitutes editorial control).

177 *See* Gillette, *supra* note 163 (explaining that after the Stratton Oakmont decision "[a] spasm of anxiety coursed through the web," since the court in Stratton Oakmont held that carriers who use "screening software to filter out offensive language and moderators to enforce guidelines," could be "held liable for the defamatory language of its users").

178 H.R. 1978, 104th Cong. (1995).

179 *Id.* § 230(c) ("No provider or user of interactive computer services shall be treated as the publisher or speaker of any information provided by an information content provider.").

180 *Id.*

181 *See* Sara L. Zeigler, *Communications Decency Act of 1996 (1996)*, THE FIRST AMEND. ENCYCLOPEDIA, https://www.mtsu.edu/first-amendment/article/1070/communications-decency-act-of-1996 ("Congress enacted the Communications Decency Act (CDA) as Title V

section 230, was signed into law by President Clinton on February 8, 1996.[182]

Section 230 of the Communications Decency Act begins by highlighting a series of "findings," which contributed to its enactment.[183] Specifically, subsection (a) discusses the rapid growth of the Internet, as well as Americans' reliance on online platforms.[184] Subsection (a)(4) additionally notes that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation."[185] Subsection (b) sets forth a "policy" that states that the country will continue to encourage the development of the Internet while ensuring Internet safety.[186] However, the key component of the legislation is found in subsection (c). Deemed "the law that matters most for speech on the web,"[187] subsection (c)(1) asserts that "[n]o 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."[188] Subsection (c) also contains a Good Samaritan provision:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> **(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> **(B)** any action taken to enable or make available to information content providers or others the

of the Telecommunications Act of 1996."); Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

182 Gillette, *supra* note 163.

183 47 U.S.C. § 230(a).

184 § 230(a).

185 § 230(a)(4).

186 § 230(b).

187 Subsection (c) establishes immunity for network operators, including social media sites. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online*, 131 HARV. L. REV. 1598, 1604 (2018).

188 47 U.S.C. § 230(c).

> technical means to restrict access to material described in paragraph (1).[189]

Since its enactment, the scope of the Communications Decency Act has been narrowed. In the 1997 case *Reno v. ACLU*, one year after the Communications Decency Act and Section 230 were enacted, the Supreme Court held that the Communications Decency Act "place[d] an unacceptably heavy burden on protected speech."[190] Specifically, the Court noted that the Communications Decency Act's ban on "indecent" content was too broad and would have a "chilling" effect on Internet speech.[191] So long as the content was not obscene, such as content depicting child pornography, it may be considered protected speech and hence could not be prohibited under the Communications Decency Act.[192] The Court's decision resulted in much of the Communications Decency Act's indecency content getting struck down,[193] resulting in a narrower application of the Communications Decency Act.

However, during that same year, the Fourth Circuit applied a broad interpretation of the Communications Decency Act and section 230 protection for providers. In *Zeran v. American Online, Inc.*, the plaintiff, Zeran, argued that AOL should have been liable for defamatory content posted on one of its forums by a third-party user.[194] Specifically, Zeran argued that AOL was aware of the defamatory content after he requested its removal and that AOL was a distributor and was consequently not protected under section 230.[195] However, the court ruled in favor of AOL because it would be "impossible" to screen millions of posts for problematic content.[196] This decision signaled that section 230 encourages a strong application in favor of network operators.[197]

189 *Id.*

190 Reno v. ACLU, 521 U.S. 844, 882 (1997).

191 *Id.* at 871–72.

192 *See id.* at 874, 883.

193 *See* Klonick, *supra* note 187, at 1605; Reno, 521 U.S. at 885 (holding that anti-indecency provisions restricted speech too much, due to the vagueness of what was considered acceptable or permissible content).

194 *See* Zeran v. American Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

195 *See id.* at 331.

196 *See id.*

197 Courts have continued to apply section 230 broadly, protecting social media companies from liability for third-party content. *See* Universal Comm. Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 415 (1st Cir. 2007) (holding that Lycos' status as an online message board "f[ell] squarely" within the immunized group protected by section 230); Nemet

More recently, the Supreme Court declined to hear a section 230 case, *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*.[198] In his statement explaining the denial of certiorari, Justice Thomas stated that "[p]aring back the sweeping immunity courts have read into section 230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place."[199] He further stated that although the Court did not hear this particular case, it would reserve the right to hear a section 230 claim in an "appropriate case."[200]

As the main statute applied in Internet liability cases, section 230 serves as one hurdle for victims of terrorist attacks and their families to bring successful claims against social media platforms. The very purpose of section 230 is to protect network providers, in this case, social media networks, from liability for third-party user content, as it is difficult to monitor every single social media post.[201] Although there are benefits of this protection,[202] section 230 should be amended to roll back immunity or implement a carve-out for terrorist content where it is clear that social media played a role in the facilitation of a terrorist attack. By modifying the scope of protection, social media companies will be held liable for this harmful content.

Chevrolet, LTD. v. Consumeraffairs.com, Inc., 591 F.3d 250, 260 (4th Cir. 2009) (holding that section 230 applied to a consumer review website).

198 The Court did not provide a reason as to why the case would not be heard. *Malwarebytes* was an antitrust case involving software developers. Malwarebytes, Inc. v. Enigma Software Group, No. 19-1284 (2020). At issue was "whether federal courts can derive an implied exception to Section 230(c)(2)(B) immunity for blocking or filtering decisions when they are alleged to be 'driven by anticompetitive animus.'" *Id.*

199 *Id.* at 9.

200 *Id.* at 10.

201 47 U.S.C. § 230.

202 *See* Jason Kelley, *Section 230 is Good, Actually*, EFF (Dec. 3, 2020), https://www.eff.org/deeplinks/2020/12/section-230-good-actually (stating that section 230 protects Big Tech and users, alike, by ensuring that social media companies are not held liable for all posts and users have the ability to post freely).

ii. The Anti-Terrorism Act Provides Civil Remedies for Victims of International Terrorism

The Anti-Terrorism Act, 18 U.S.C. § 2333, was first enacted in 1990.[203] The Act established "a new civil cause of action in Federal law for international terrorism that provide[d] extraterritorial jurisdiction over terrorist acts abroad against United States nationals."[204] The Anti-Terrorism Act was proposed in response to two international terrorist attacks against American citizens: the bombing of Pan Am Flight 103 and the murder of American citizen Leon Klinghoffer.[205]

On December 21, 1988, Pan Am Flight 103 departed London Heathrow Airport for New York City.[206] One hundred ninety Americans were on board the flight.[207] Less than forty minutes after departure, the plane exploded 30,000 feet above Lockerbie, Scotland, killing everyone on board and eleven people on the ground.[208] The FBI, in conjunction with international law enforcement from Germany, Austria, Switzerland, and Great Britain, discovered that a bomb had been placed inside a radio in a piece of luggage that was detonated during the flight.[209] In November 1991, the United States and Scotland indicted two Libyan intelligence operatives for planting the bomb.[210] On January 31, 2001, Abdel Basset Ali Al-Megrahi was found guilty of the attack.[211] Additionally, the Libyan government accepted responsibility for the attack and agreed to pay the victims' families approximately three billion dollars.[212]

On October 7, 1985, three years before the Pan Am attack, four members of the Palestine Liberation Front (PLF) hijacked an

---

203 S. 2465, 101st Cong. (1990).

204 *Id.*

205 102 CONG. REC. S4511 (1991).

206 *Pan Am 103 Bombing*, FBI.GOV, https://www.fbi.gov/history/famous-cases/pan-am-103-bombing (last visited Jan. 15, 2022).

207 *Id.* ("Among the 259 passengers and crew were 190 Americans.").

208 *Id.*

209 *See id.* (explaining that after investigating 845 square miles of Scotland and interviewing more than 10,000 individuals, law enforcement was able to piece together the tools used in the terrorist attack).

210 *Id.*

211 *Id.* (explaining that al-Megrahi was convicted but his co-defendant was found not guilty and released).

212 *Id.*

Italian cruise ship, the *Achille Lauro*, and took 400 passengers hostage.[213] American and British passengers were separated from the rest of the ship and told that they would be killed if they did not comply with the hijackers' demands.[214] Upon approaching Damascus, the hijackers demanded to be connected to American and Italian authorities to negotiate the release of fifty prisoners being held in a prison in Israel.[215] When their demands were not met, the hijackers separated sixty-nine-year-old American citizen, Leon Klinghoffer, from his wife and the rest of the group.[216] Through eyewitness reports and radio transmissions from the hijackers to a Lebanese radio station, authorities discovered that the hijackers had shot and killed Mr. Klinghoffer.[217] The hijacking lasted two days and concluded when the secretary-general of the PLF, Mohammed Abbas Zaidan, urged the hijackers to surrender in exchange for safe passage out of Egypt.[218] The hijackers complied and were transported off the ship.[219]

In 1991, Ilsa and Lisa Klinghoffer, Leon Klinghoffer's daughters, filed a lawsuit against the Palestinian Liberation Organization (PLO) for the death of their father.[220] The Anti-Terrorism Act was applied in that case, providing American jurisdiction over the PLO.[221] However, nearly five months after its enactment, the Anti-Terrorism Act was repealed due to a technical

213 Jennifer Latson, *A Murder That Shocked the World, at Sea and on Stage*, TIME (Oct. 7, 2015, 10:30 AM), https://time.com/4055773/achille-lauro/ (discussing the significant impacts of this attack); William E. Smith, *Terrorism: The Voyage of the Achille Lauro*, TIME (Oct. 21, 1985), http://content.time.com/time/subscriber/article/0,33009,960163-1,00.html (according to the Italian News Agency, ANSA, the men had intended to quietly board the ship at Genoa and launch a terrorist attack at the Ashdod port but their plan drastically changed after waiters on board the ship saw the men cleaning their guns).

214 *See* Smith, *supra* note 213.

215 *Id.*

216 *Id.*

217 *Id.*

218 *Id.*

219 *Id.* ("Shortly before dusk Wednesday, the four gunmen came ashore aboard a squat, battered tugboat of the Suez Canal Authority. Then they disappeared, not to resurface until they landed in Sicily some 30 hours later.").

220 *See* Klinghoffer v. S.N.C. Achille Lauro, 937 F.2d 44, 44 (2d Cir. 1991) (holding that the PLO was not "immune from suit," despite claims that the United States lacked jurisdiction over the matter); Klinghoffer v. S.N.C. Achille Lauro, 739 F. Supp. 854, 854 (S.D.N.Y. June 7, 1990).

221 *See Klinghoffer*, 937 F.2d at 865 (citing United States v. Palestine Liberation Org., 695 F. Supp. 1456, 1461 (S.D.N.Y. 1988) (concluding that the ATA granted jurisdiction over the PLO)).

error.[222] Due to its significant role in impending litigation, as well as the unanimous support provided during the first enactment, the Anti-Terrorism Act was reintroduced and passed again in 1991.[223]

The Anti-Terrorism Act provides civil remedies for "[a]ny national of the United States injured . . . by reason of an act of international terrorism."[224] Specifically, section (a) of the Anti-Terrorism Act states that,

> Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees.[225]

In 2016, the Anti-Terrorism Act was expanded through the Justice Against Sponsors of Terrorism Act (JASTA).[226] JASTA expanded the scope of potential claims by adding civil liability for individuals or organizations accused of aiding and abetting terrorist organizations.[227] As stated by Senator Chuck Grassley, the original sponsor of the Anti-Terrorism Act, "[t]he ATA removes the jurisdictional hurdles in the courts confronting victims and it empowers victims with all the weapons available in civil litigation."[228]

The Anti-Terrorism Act has since been applied in multiple cases involving terrorism and banking institutions.[229] However, in the

---

222 *See* 102 CONG. REC. S4,511 (1991) ("Due to an enrolling error, the ATA was enacted into law on November 5, 1990[,] as part of the Military Construction Appropriations Act—Public Law 101-519. . . . Unfortunately, this law was repealed just a few weeks after oral argument; albeit, on purely technical grounds.").

223 *See id.* ("The ATA garnered strong bipartisan support in both the House and Senate. . . . [T]he Senate unanimously supports the ATA.").

224 18 U.S.C. § 2333(a).

225 *Id.*

226 *See Justice Against Sponsors of Terrorism Act: Hearing Before the Subcomm. on the Const. & Civ. Just. Of the Comm. On the Judiciary H.R.*, 114th Cong. 114-87 (2016) ("JASTA amends the Antiterrorism Act to clarify that those who aid, abet, or conspire with a foreign terrorist organization are subject to civil liability.").

227 *See* Justice Against Sponsors of Terrorism Act of 2016, Pub. L. No. 114-222, § 2(b) (2016).

228 102 CONG. REC. S4511 (1991).

229 *See, e.g.*, Jesner v. Arab Bank, PLC, 138 S. Ct. 1386, 1393–394 (2018) ("It is assumed here that those individuals who inflicted death or injury by terrorism committed crimes in

field of terrorism and social media, Anti-Terrorism Act claims have been largely unsuccessful.[230] Currently, the Sixth and Ninth Circuits have dismissed Anti-Terrorism Act social media claims.[231] However, many similar cases of this nature are to be expected, which may ultimately lead to new case law.[232]

Thus far, two district courts have ruled in Anti-Terrorism Act social media cases.[233] *Pennie v. Twitter*, a 2017 case from California, was one of the first cases to apply the Anti-Terrorism Act in the context of social media terrorism.[234] On July 7, 2016, Hamas sympathizer Micah Johnson murdered five police officers in Dallas, Texas.[235] The victims' families and fellow police officers sued Twitter, Google, and Facebook, alleging that the platforms aided and abetted the attack, thus violating the Anti-Terrorism Act, by maintaining Hamas social media profiles.[236] The court dismissed the claims, alleging that the Plaintiffs failed to establish proximate cause under the Anti-Terrorism Act.[237] Even though Johnson had "liked" several extremist pages, the Plaintiffs could not prove that Hamas had directly contacted Johnson or that he viewed any of their content.[238] Likewise, in the 2018 case *Taamneh v. Twitter*, the court dismissed the Plaintiffs' Anti-Terrorism Act claim regarding an ISIS terrorist attack in an

violation of well-settled, fundamental precepts of international law, precepts essential for basic human rights protections. It is assumed as well that individuals who knowingly and purposefully facilitated banking transactions to aid, enable, or facilitate the terrorist acts would themselves be committing crimes under the same international-law prohibitions."). This note does not discuss the ATA in connection with financial institutions.

230 *See* Y. Peter Kang, *6th Circ. Ruling Raises Bar For Social Media Terrorism Suits*, LAW 360 (Apr. 19, 2019), https://www.law360.com/articles/1151658/6th-circ-ruling-raises-bar-for-social-media-terrorism-suits ("[The Anti-Terrorism Act] makes it very hard for plaintiffs to come up with facts to get around the rulings. The writing is on the wall that [these suits] have a very low chance of success.").

231 *See id.* ("The Sixth Circuit's published opinion cites the Ninth Circuit's January 2018 precedential ruling in Fields v. Twitter Inc., which held that the social media company couldn't be held liable for a 2015 Islamic State attack in Jordan that killed two government contractors."); Crosby v. Twitter Inc., 921 F.3d 617, 628 (6th Cir. 2019) (dismissing claims for failure to show proximate cause); Fields v. Twitter Inc., 881 F.3d 739, 741 (9th Cir. 2018) (dismissing claims for failure to show proximate cause).

232 *See* Kang, *supra* note 230, at 2 (explaining that as terrorism continues to maintain a presence on social media, scholars predict that parties will continue to utilize the ATA as a possible route for civil remedies).

233 *See generally* Pennie v. Twitter, Inc., 281 F. Supp. 3d 874 (N.D. Cal. 2017); Taamneh v. Twitter, Inc., 343 F. Supp. 3d 904, 907 (N.D. Cal. 2018).

234 *See Pennie,* 281 F. Supp. 3d at 877.

235 *See id.* at 876–77.

236 *See id.* at 877.

237 *See id.* at 886.

238 *See id.* at 888.

Istanbul nightclub.[239] The court in *Taamneh* similarly dismissed the claim for failing to establish the proximate cause element.[240] The court also dismissed the claim because the plaintiffs failed to prove that the defendants committed an "act of international terrorism," pursuant to the statute.[241]

This rationale for dismissal was further affirmed in two separate cases, which reached the Ninth and Sixth Circuits, respectively. In the 2018 case *Fields v. Twitter*, family members of deceased government contractors murdered by a Jordanian police officer who had pledged allegiance to ISIS sued Twitter for enabling the distribution of propaganda and facilitating direct messaging between the police officer and ISIS.[242] The Ninth Circuit dismissed the claim, determining that the Plaintiffs failed to show proximate causation.[243] Namely, the Plaintiffs failed to prove that Twitter's conduct *directly* caused the attack to occur.[244] Likewise, in *Crosby v. Twitter*, the Sixth Circuit dismissed all Anti-Terrorism Act claims regarding the Pulse Nightclub shooting in 2016.[245] The court held that the Plaintiffs failed to prove that Twitter proximately caused the attack because extremist content on social media does not necessarily lead to direct radicalization.[246] Furthermore, the court held that since Twitter did not physically commit the act of terrorism, it was not liable for the execution of the attack.[247] Finally, the court emphasized that

239 *See Taamneh*, 343 F. Supp. 3d at 877.

240 *See id.* at 911 (stating that the Plaintiffs failed to show that the terrorist saw content published by ISIS and that the Plaintiffs failed to show that the Defendants were knowingly aiding and abetting a terrorist cause).

241 *See id.* (explaining that the Anti-Terrorism Act provides civil remedies for acts of international terrorism against United States nationals, and where terrorism occurs on United States soil or does not meet the full definition of international terrorism, pursuant to 18 U.S.C. § 2331, parties cannot recover on an ATA claim).

242 *See generally* Fields v. Twitter, Inc., 881 F.3d 739, 741 (9th Cir. 2018).

243 *See id.* (explaining that the Plaintiffs failed to show a direct connection between social media consumption and the execution of a terrorist attack).

244 *See id.* at 748–51 (noting that although the suspect might have viewed extremist content, the Plaintiffs could not show that the Defendants' content served as the critical force in his decision to execute the attack).

245 *See* Crosby v. Twitter, Inc., 921 F.3d 617, 626 (6th Cir. 2019).

246 *See id.* at 624–25.

247 *See id.* at 627.

the attack was not international and therefore, not subject to the protection of the Anti-Terrorism Act.[248]

The Anti-Terrorism Act places burdensome restrictions on parties seeking to bring claims against social media platforms for their involvement in facilitating terrorism. Specifically, barring claims of domestic terrorism arbitrarily discriminates against victims of domestic terrorist attacks and their families; it also forces judges to become experts in national security when determining whether an attack constitutes international terrorism. Accordingly, the Anti-Terrorism Act should be amended to expand the scope of claims that can be raised by victims.

II. SECTION 230 AND THE ANTI-TERRORISM ACT SHOULD BE AMENDED TO ALLOW SOCIAL MEDIA PLATFORMS TO BE HELD LIABLE FOR THE PUBLICATION OF TERRORIST CONTENT

Social media terrorism is a significant problem that threatens national security. Given the rapid evolution of terrorism, it is critical for platforms to not only keep up with mitigating the threat but stay ahead of it. To accomplish this important policy goal, section 230 of the Communications Decency Act and the Anti-Terrorism Act should be amended to hold social media companies liable where a failure to act results in the clear planning, organizing, or execution of an attack.[249] First, section 230 needs to be amended to roll back the broad immunity afforded to network operators. This amendment would implement consequences for platforms regarding social media terrorism and enable victims to bring lawsuits against social media companies. Second, the Anti-Terrorism Act needs to be amended to include recourse for victims of domestic terrorist attacks. By enacting these amendments,

248 *See id.* at 621 (noting that domestic terrorism is not recognized by the Anti-Terrorism Act. Therefore, since the act occurred in Orlando by an American gunman, a claim could not be brought under the Anti-Terrorism Act).

249 47 U.S.C. § 230. To reiterate, this standard would encourage liability in situations where individuals or organizations openly discussed plans of violence or clearly intended to commit an organized, harmful act. Evidence might include open communication between an individual and an organization, unremoved posts of violence or threats, consistent or increased engagement with organizations or ideologies, etc.

either separately or in conjunction with one another, victims would have greater legal recourse following an act of terrorism.

A. Section 230 Should be Amended to Remove Broad Immunity for Network Operators, to Allow Victims of Social Media Driven Attacks to File a Lawsuit

Since its enactment, section 230 has been scrutinized for the "sweeping immunity"[250] it provides to network operators, especially social media sites. Accordingly, calls to amend section 230, specifically proposals to roll back the scope of immunity, are justified because the current framework absolves social media companies of all responsibility for social media terrorism, even when a platform has clearly failed to investigate and remove suspect content.

Section 230 should be amended to account for the evolving safety and security needs of society. Section 230 was proposed in 1995 and was intended to protect individuals, namely minors, from viewing offensive content via media outlets.[251] At the time of the proposal, social media was in its early stages and many of today's concerns and threats were not yet recognized. Additionally, section 230 was enacted before September 11, 2001. While the United States had suffered terrorist attacks before September 11,[252] the threat, danger, and complexity of future attacks were likely not yet realized.[253] Accordingly, section 230 should be amended to provide a "carve-out" for terrorism to reflect the realistic threats seen today and further incentivize social media

250 Malwarebytes, Inc. v. Enigma Software Group, No. 19-1284 (2020) (discussing section 230's broad immunity).

251 47 U.S.C. § 230.

252 By the time section 230 was proposed, the United States had experienced the 1993 World Trade Center bombing. BUREAU OF DIPLOMATIC SECURITY, *1993 World Trade Center Bombing*, U.S. DEP'T OF ST. (Feb. 21, 2019), https://www.state.gov/1993-world-trade-center-bombing/.

253 *See 9/11 Investigation*, FBI, https://www.fbi.gov/history/famous-cases/911-investigation (last visited Jan. 23, 2022) ("They were the most lethal terrorist attacks in history, taking the lives of 3,000 Americans and international citizens and ultimately leading to far-reaching changes in anti-terror approaches and operations in the U.S. and around the globe."); *Explosions at Boston Marathon*, NPR, https://www.npr.org/series/177378595/boston-marathon-explosions (last visited Jan. 23, 2022); *Orlando Shooting*, N.Y. TIMES (June 20, 2016), https://www.nytimes.com/news-event/2016-orlando-shooting.

companies to take a stronger stance on extremist content. Unlike previous applications where companies were shielded from defamation lawsuits,[254] social media terrorism is a matter of national security. Therefore, protecting "Big Tech" companies should not outweigh the importance of holding those companies accountable for failing to act and prevent national security disasters.

The current state of section 230 also deprives victims and their families of the opportunity to have their day in court. As stated by Justice Thomas, the widespread immunity offered by section 230 denies plaintiffs the chance to bring a claim against network operators from the start, regardless of the merits of the case.[255] This is unjust as victims of terrorist attacks and their families should be able to seek legal redress if it is found that social media played a role in the execution of an attack.[256] Some may argue that amending section 230 would not significantly impact the scope of legal redress available because of other hurdles, such as proximate cause. Specifically, even if an amendment narrowed immunity, plaintiffs would still bear the burden of proving that the social media platform directly caused the attack. While that may be true, it should not restrict a victim or family's ability to file a lawsuit from the outset. For example, social media records clearly displayed posts advocating for the Capitol insurrection, including discussions of violence.[257] Despite the overwhelming evidence on social media that reflects many platforms' failure to act and stop conversations referencing violence and insurrection, a victim or their family would not be able to sue any social media companies.

Accordingly, section 230's broad immunity absolves network operators of liability for the content published on their sites, regardless of the potentially damaging effect on victims, families,

254 *See* Zeran v. American Online, Inc., 129 F.3d 327 (4th Cir. 1997) (involving claims of defamation and libelous content).

255 Malwarebytes, Inc. v. Enigma Software Group, No. 19-1284, (2020); Crosby v. Twitter Inc., 921 F.3d 617, 628 n. 7 (6th Cir. 2019) ("Even if ISIS 'committed, planned, or authorized' the Pulse Night club shooting, Plaintiffs would still have to overcome 47 U.S.C. § 230, which provides broad immunity to 'interactive computer services.' This is another substantial hurdle for Plaintiffs.").

256 *See* 18 U.S.C. § 2333. This may include records of direct engagement, content posted by the terrorists, manifestos or documents signaling an intent to act, or other clear evidence of participation. *See Foreign Terrorist Organizations*, *supra* note 135.

257 *See* Collins & Zadrozny, *supra* note 5 (discussing social media posts advocating for the Capitol insurrection).

and the nation. While the hope is that social media platforms will self-regulate the content, there is no legal recourse if such mechanisms fail. By rolling back section 230 protection and increasing accountability of social media platforms, victims would be given an avenue of recourse and social media companies would be further incentivized to continuously revise and update their policies.

The goals of this proposed rollback are to increase accountability where social media has clearly assisted in the planning, growth, and organization of an attack. However, calls to completely repeal section 230 may do more harm than good. Section 230 protects social media platforms from a flood of litigation, specifically by preventing claims about content that is not objectively offensive or harmful. Therefore, a balance must be struck to ensure that social media platforms do not lose all protection, while also ensuring that they do not receive the form of "qualified immunity" that has existed for so long.

B. The Anti-Terrorism Act Should be Amended to Include Instances of Domestic Terrorism, to Expand the Scope of Claims that can be Brought Under the Anti-Terrorism Act

The Anti-Terrorism Act was enacted to provide civil remedies for American victims of international terrorist acts by enabling victims and their families to hold perpetrators liable for their deadly crimes.[258] Although a significant Act for victims of terrorism, the Anti-Terrorism Act fails to account for terrorism's evolving nature. The Anti-Terrorism Act places burdensome restrictions on legal claims, thereby preventing parties from recovering from all types of terrorist attacks.[259] Therefore, the Anti-Terrorism Act should be amended to include both

258 *See* S. 2465, 101st Cong. (1990).

259 *See id.* Compiling the case law of ATA cases shows that the two largest obstacles for plaintiffs include proving proximate cause and proving acts of international terrorism. This note will not address proving proximate cause, as such proof would likely be difficult to obtain because the proximate cause is measured with respect to the content's direct impact on the perpetrator. *See* Fields v. Twitter Inc., 881 F.3d 739, 741 (9th Cir. 2018). However, amending the ATA to recognize domestic claims, in addition to international terrorism claims, would potentially expand the scope of recovery for victims of domestic terror attacks.

international and domestic terrorist attacks to expand the possible scope of claims and provide legal recourse for victims of terrorist attacks and their families. Although the Anti-Terrorism Act would not directly impact social media companies, it would provide an additional avenue of recovery against domestic actors who utilized social media for the execution of an attack.

The Anti-Terrorism Act was originally enacted in 1990, before the growth of social media and the first terrorist attacks on United States soil.[260] Similar to section 230, this is a problem because legislators were not aware of events that would transpire in the future, specifically the dominance of social media and the complexity of modern terrorism.[261] Almost twenty years ago, the nation experienced "the most lethal terrorist attacks in history."[262] Critical actions were taken to combat the new world threat.[263] With the threat of domestic terrorism growing and no current, widespread legislation in place to prosecute domestic terrorists, the Anti-Terrorism Act must be amended to proactively combat this danger.

Domestic terrorism is a significant threat to national security. Currently, experts believe that domestic terrorism accounts for twenty percent of all terrorism threats.[264] From 2017 to 2019, the United States made more domestic terrorism-related arrests than international terrorism-related arrests.[265] Specifically, in 2018, all "extremism-related murders" were committed by "right-wing domestic terrorists."[266] Additionally, as stated by Brian Murphy, former Principal Deputy Under Secretary for the Office of Intelligence and Analysis in DHS, "lone actors from [domestic terrorism] movements pose the greatest threat to the homeland

260 *See* S. 2465, 101st Cong. (1990); *1993 World Trade Center Bombing*, *supra* note 252.

261 *See 9/11 Investigation, supra* note 253. Pre-September 11, the nation was not completely aware of the severity of international terrorism. *See id.* More than thirty years after the ATA's enactment, the threat of international terrorism remains, in addition to the rise of domestic terrorism. *See* Jones et al., *supra* note 149, at 1. Accordingly, the scope and complexity of terrorism have grown exponentially. *See id.* at 6.

262 *See 9/11 Investigation*, *supra* note 253 (describing September 11, 2001).

263 *See* DHS, *September 11 Chronology*, DEP'T OF HOMELAND SEC. (Sept. 3, 2020), https://www.dhs.gov/september-11-chronology (discussing the actions taken after 9/11, including the creation of DHS).

264 *See* Jones et al., *supra* note 149.

265 *Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the Comm. on Homeland Sec.*, 116th Cong. 1–2 (2019) (statement of Hon. Bennie Thompson, Chairman, H. Comm. on Homeland Sec.).

266 *Id.*

due to their ability, in many instances, to remain undetected by law enforcement."[267] Although agencies have cooperated with social media companies to track the threat of domestic terrorism, many companies are not yet equipped to properly detect and neutralize threats.[268] Accordingly, with so much uncertainty surrounding such a pressing threat, the Anti-Terrorism Act should be amended to provide one option of legal recourse for domestic terrorism victims. Although other obstacles may not guarantee judgment in favor of a victim or their family, domestic terrorism claims would not be "barred" outright by the Anti-Terrorism Act.[269]

Enabling both international and domestic terrorism claims would also show the legitimacy of the threat of domestic terrorism in the United States. The current system is flawed if only victims and families of international attacks can recover damages, whereas those who suffered from a domestic attack, such as the Pulse Nightclub attack, cannot. Additionally, as openly recognized by public officials, there is less transparency and education regarding domestic terrorism.[270] By expanding the scope of the Anti-Terrorism Act, greater attention would be brought to the threat of domestic terrorism and the uncertainty surrounding it. Both international and domestic attacks are forms of terrorism, regardless of who committed them or where they occurred. Accordingly, by expanding the designation, victims and their families would be afforded an improved opportunity to bring claims against domestic terrorists.

In addition to the importance of justice for victims and their families, an amendment to the Anti-Terrorism Act is an important policy decision. Much of the line between international and domestic terrorism has been "blurred."[271] When designating a terrorist attack as international or domestic, officials will typically

---

267 *Id.* at 19–20 (statement of Brian Murphy, Principal Deputy Under Secretary for the Off. of Intelligence and Analysis in the Dep't of Homeland Sec.).

268 *Id.* at 17 (statement of Michael McGarrity, Assistant Dir. for the Counterterrorism Div., Federal Bureau of Investigation, U.S. Dep't of Just.).

269 18 U.S.C. § 2333 (stating that recovery is available for international terrorist attacks).

270 *Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 2 (2019) (statement of Hon. Bennie Thompson, Chairman, H. Comm. on Homeland Sec.).

271 *See generally* Gregory D. Miller, *Blurred Lines: The New "Domestic" Terrorism*, 13 PERSP. ON TERRORISM 63, 63 (June 2019).

consider three factors: the nationality of the terrorist(s), the nationality of the victim(s), and the location of the crime.[272] However, it is unclear how those factors must align to determine whether an attack is deemed international or domestic.[273] In the context of social media, there can be even greater uncertainty as to how to classify an attack. For example, if an American citizen becomes radicalized through social media by an influence or cause that is "foreign" to their home, it remains a question of what impact that would have on classification as a domestic or international attack.[274] By expanding the Anti-Terrorism Act to account for both forms of terrorism, the courts will not set a dangerous precedent in determining which acts constitute strictly international terrorism and which represent solely domestic attacks. Enabling both claims essentially makes the litigation process easier by not having judges serve as experts on matters of national security. Additionally, these claims advance overall safety and security by ensuring that all terrorist attacks are properly investigated and litigated.

In conjunction with an amendment to the Anti-Terrorism Act, social media platforms must also work to expand and improve their removal policies regarding domestic terrorism. In 2019, social media companies were still working to "improve" their regulation of domestic terrorism.[275] In improving their methods and policies, social media platforms should compile a list of suspect organizations, as well as common hashes used by those organizations, that suggest inciting violence or an imminent threat of attack. This would create a uniform regulatory system and prevent social media sites from only recognizing international organizations or being divided on which groups are considered domestic terrorists. Through both legislative amendments and a

272 *See id.* at 64 (explaining that the Oklahoma City bombing was classified as a domestic attack because American citizen Timothy McVeigh executed an attack against Americans in the United States, whereas 9/11 was an international attack as it was executed by a non-citizen against Americans in the United States).

273 *See id.*

274 *See id.* at 68.

275 *Confronting the Rise of Domestic Terrorism in the Homeland: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 32 (2019) (statement of Michael McGarrity, Assistant Dir. for the Counterterrorism Div., Federal Bureau of Investigation, U.S. Dep't of Jus.).

"boots on the ground" approach by social media companies, internet safety would improve.

Some might argue that increased scrutiny of content to mitigate the spread of terrorism would lead to censorship and First Amendment violations. Although the First Amendment does not apply to private social media sites,[276] freedom of speech and expression is a critical aspect of social media. However, social media regulatory policies would still be in place to investigate potential errors in removal.

Although additional legislation has been enacted to address terrorism, the Anti-Terrorism Act has remained unchanged regarding the scope of recovery for victims of international terrorist attacks.[277] This is a critical issue, as the sole statute for civil redress has failed to account for the rapidly progressing nature of terrorism. By expanding the scope of the Anti-Terrorism Act, greater attention would likely be placed on the growing threat of domestic terrorism, and victims of domestic terrorism and their families would have a better opportunity for legal redress.

CONCLUSION

Terrorism is a severe threat to the United States—and its presence is closer than most Americans suspect. If policies and regulatory methods remain stagnant, despite advancements in technology, terrorism will only continue to grow. However, the regulation and prevention of terrorism can be achieved by amending current federal legislation. Amending section 230 and

276 The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." U.S. CONST. amend. I. The First Amendment of the United States Constitution is often cited by social media users as justification for the content of online posts. *See* David L. Hudson, Jr., *In the Age of Social Media, Expand the Reach of the First Amendment*, HUM. RTS. MAG. (Oct. 2018). Accordingly, social media users often use the First Amendment to justify the content of their posts and further argue against the removal of that content. *See id.* at 2. However, the First Amendment applies only to state action and not that of private companies. *See id.* at 3. Hence, the First Amendment currently does not protect users' speech on privately-owned social media platforms. *See id.* at 2.

277 *See generally* 18 U.S.C. § 2333; 18 U.S.C. §§ 2331–2339 (explaining the applicable terrorism statutes).

removing some immunity provided to social media platforms will allow plaintiffs to bring claims before the courts. Furthermore, amending the Anti-Terrorism Act and incorporating domestic terrorist attacks will give victims of domestic terrorism attacks an added layer of support in raising claims against social media companies. Accordingly, such steps should be taken to ensure justice for victims and ensure the regulation of social media terrorism.