Pepperdine Law Review

Volume 46 | Issue 1 Article 4

1-15-2019

When You Give a Terrorist a Twitter: Holding Social Media Companies Liable for Their Support of Terrorism

Anna Elisabeth Jayne Goodman
J.D. Candidate, Pepperdine University School of Law

When You Give a Terrorist a Twitter: Holding Social Media Companies Liable for Their Support of Terrorism

Abstract

In the electronic age, the internet—and—social media specifically, can be a tool for good but, abused and unchecked, can lead to great harm. Terrorist organizations utilize social media as a means of recruiting and training new members, urging them to action, and creating public terror. These platforms serve as the catalyst for equipping the growing number of "lone wolf" attackers taking action across the United States. Under civil liability provisions created under JASTA and the ATA, material supporters of terrorism can be held liable for their actions, and with the key role social media sites now play in supporting terrorism, they should certainly be subjected to liability under this provision. Conflicting case law regarding causation and the "internet provider shield" provided by section 230 of the Communications Decency Act have largely precluded this liability to date. However, national security and counter-terror concerns counsel application of liability in the social media context, and an analysis of the law shows that it could be done without infringing in any way on the rights guaranteed under the First Amendment. Through both judicial and legislative means, changes can be made to create greater responsibility for these social media companies in the future, fostering an environment that will help to limit the currently increasing number of social media-incited attacks and hold social media companies appropriately responsible when their actions are the catalyst for a significant loss of life.

TABLE OF CONTENTS

I. INTRODUCTION

December 2, 2015*: Syed Rizwan Farrook and Tashfeen Malik walked into an office Christmas party in San Bernardino and opened fire, killing fourteen partygoers and injuring at least twenty-one others.*[1] *Hours before the attack, they pledged allegiance to the Islamic State on social media.*[2]

June 12, 2016*: Omar Mateen walked into Orlando's Pulse nightclub and shot fifty people to death, injuring many more in the process.*[3] *He used Facebook to track unfolding events during the attack.*[4]

October 31, 2017*: Uzbek immigrant Sayfullo Saipov drove his truck onto a busy Manhattan bike path, killing eight people.*[5] *FBI investigators found ninety ISIS social media propaganda videos on his phone.*[6]

With acts of independent "lone-wolf" terrorism on the rise across the western world, the pressing question of what is causing this emergent trend—and how to combat it—has pushed scholars and law enforcement alike to pursue an aggressive search for answers.[7] This search has revealed that these so-called "lone-wolf" attackers are not so alone after all.[8] Alt-

1. Camila Domonoske, *San Bernardino Shootings: What We Know, One Day After*, NPR (Dec. 3, 2015, 6:47 AM), https://www.npr.org/sections/thetwo-way/2015/12/03/458277103/san-bernardino-shootings-what-we-know-one-day-after.

2. *Everything We Know About the San Bernardino Terror Attack Investigation So Far*, L.A. TIMES (Dec. 14, 2015, 4:03 PM), http://www.latimes.com/local/california/la-me-san-bernardino-shooting-terror-investigation-htmlstory.html.

3. David Smith et al., *Orlando: Obama Condemns 'Act of Terror' After Worst Mass Shooting in US History*, GUARDIAN (June 12, 2016, 4:12 PM), https://www.theguardian.com/us-news/2016/jun/12/orlando-terror-attack-50-killed-nightclub-deadliest-mass-shooting.

4. David Smith & Spencer Ackerman, *Orlando Gunman Searched for Facebook Reaction During Pulse Nightclub Attack*, GUARDIAN (June 16, 2016, 1:02 PM), https://www.theguardian.com/us-news/2016/jun/16/orlando-attack-facebook-post-pulse-nightclub-shooting; *see* Ariel Zambelich & Alyson Hurt, *3 Hours in Orlando: Piecing Together an Attack and Its Aftermath*, NPR (June 26, 2016, 5:09 PM), https://www.npr.org/2016/06/16/482322488/orlando-shooting-what-happened-update.

5. David Patrikarakos, *Social Media Networks are the Handmaiden to Dangerous Propaganda*, TIME (Nov. 2, 2017), http://time.com/5008076/nyc-terror-attack-isis-facebook-russia/.

6. *Id.*

7. Daniel L. Byman, *How to Hunt a Lone Wolf: Countering Terrorists Who Act on Their Own*, BROOKINGS (Feb. 14, 2017), https://www.brookings.edu/opinions/how-to-hunt-a-lone-wolf-countering-terrorists-who-act-on-their-own/. Lone-wolf terrorists are politically motivated attackers who act alone. *See* Katie Worth, *Lone Wolf Attacks Are Becoming More Common—And More Deadly*, FRONTLINE (July 14, 2016), https://www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

8. *See* Jen Easterly & Joshua A. Geltzer, *The Islamic State and the End of Lone-Wolf Terrorism*,

hough they come from all walks of life and all types of communities, these attackers share one significant habit in common: their use of social media.[9] Over the past few years, Facebook, Twitter, Instagram, and similar platforms have become the primary means utilized by extremist groups to recruit, educate, and ultimately, equip their followers to go and kill.[10] It is well-established that, under U.S. law, terrorists are subject to civil liability for their actions—and so are those that support them.[11] In light of the advent and exponential growth of social media use by terrorist actors, the legal community now faces a new question of if, and when, the companies facilitating online terrorist communication should face liability for *their* contributions to terrorism.[12]

This Comment recognizes the complicated dynamics and policy implications of holding social media companies civilly liable as supporters of international terrorism, posits that this may be done effectively, and offers suggestions for the best way to address such cases, both in the present and

---

FOREIGN POL'Y (May 23, 2017, 12:56 PM), http://foreignpolicy.com/2017/05/23/the-islamic-state-and-the-end-of-lone-wolf-terrorism/ ("The Islamic State hasn't unleashed lone-wolf terrorism; instead, its unique manipulation of modern communications technologies portends the end of lone-wolf terrorism.").

9. *See generally* Brendan I. Koerner, *Why ISIS Is Winning the Social Media War*, WIRED (Apr. 2016), https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/ (articulating how the Islamic State has successfully used social media to propagate terrorism). This Comment uses a variety of examples of "lone wolf" attacks that have occurred in the United States and internationally over the past few decades; many of these focus on attacks motivated by Al-Qaeda and ISIS. However, these are simply examples based on recent events. The scope of this paper is in no way limited to one terrorist organization or ideology and these examples are simply useful to illustrate the impact of extremist group's social media use, *see infra* Part II, and the need for legal accountability for the websites enabling them to achieve their goals, *see infra* Parts III–V.

10. *See* Koerner, *supra* note 9. Today, terrorist organizations affirmatively pursue recruits via social media. *See* Pamela Engel, *Here's the Manual That Al-Qaeda and Now ISIS Use to Brainwash People Online*, BUS. INSIDER (July 2, 2015, 11:45 AM), http://www.businessinsider.com/the-manual-al-qaeda-and-now-isis-use-to-brainwash-people-online-2015-7. These techniques have become such a central part of recruitment methods for ISIS and Al-Qaeda that they have even been codified in a recruitment manual. *See id.*

11. *See* discussion *infra* Part III. Supporting terrorism also subjects supporters of terrorism to criminal liability; however, that is not the focus of this Comment. *See* Alexander Tsesis, *Social Media Accountability for Terrorist Propaganda*, 86 FORDHAM L. REV. 605, 625–28 (2017) (discussing the types of liability to which social media companies may be subjected).

12. *See* Tsesis, *supra* note 11, at 619 (explaining the federal government's reluctance in holding social media companies liable for materially supporting terrorism and its ability to restrict a company's free speech rights). "[W]here Twitter, Facebook, YouTube, and similar content carriers receive notice of terrorist statements that harmed or are likely to result in attacks against a party, a court should find standing for a plaintiff to proceed with a civil suit for compensatory, injunctive, or punitive relief." *Id.* at 625.

the long-term.[13] Part II explains the relationship between social media use and terrorism.[14] Part III explores the Anti-Terrorism Act's (ATA) role as a source of civil liability for social media platforms utilized by terrorists.[15] Meanwhile, Part IV discusses the challenges to imposing such liability caused by the Communications Decency Act (CDA),[16] while Part V addresses the competing interests of national security and free speech, the two most significant policy concerns implicated by imposing civil liability on social media providers.[17] Finally, Part VI turns the focus to the future, considering the best means for pursuing civil action against social media companies under the current laws and suggesting legislative changes to improve these conduits in the future.[18] There is a point at which social media companies must be held liable for their contributions to terrorism.[19] Increased litigation and improved legislation would be an invaluable asset in the fight against terrorism, requiring a heightened level of accountability from the companies who currently enable these horrific attacks and offering a clearer means of recovery for the victims who suffer as a result of them.[20]

II. UNDERSTANDING THE RELATIONSHIP BETWEEN SOCIAL MEDIA AND TERRORISM

Beginning shortly after 9/11, web use by terrorists skyrocketed.[21] Traditional websites and discussion forums initially provided the primary online means for promoting terrorist agendas.[22] However, the rapid evolution of the internet over the past decade and a half facilitated the development of an environment particularly suited to the needs and goals of terrorist actors and organizations, leading members of these groups—along with the general populace—to increasingly abandon a more traditional website structure in favor of the new, interactive, and self-initiating: social media sites.[23] The

13. *See infra* notes 14–18 and accompanying text.
14. See *infra* Part II.
15. *See infra* Part III.
16. *See infra* Part IV.
17. *See infra* Part V.
18. *See infra* Part VI.
19. *See infra* discussion Parts III–VI.
20. *See infra* Part VI.
21. Gabriel Weimann, *New Terrorism & New Media*, COMMONS LAB 2 (2014), https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F_0.pdf.
22. *See id.*
23. *See* Nina I. Brown, *Fighting Terror, Not Twitter: Insulating Social Media from Material*

advent and rapid growth of social media provided new avenues for information dissemination, connectivity, and interactive communication that terrorists quickly recognized as a far superior means for recruitment, radicalization, and fearmongering.[24] Today, social media sites are the hub for more than ninety percent of the organized terrorism efforts conducted via the internet.[25] Scholars recognize that terrorist actors' strategies for using social media communication networks "are nearly as creative and quick to develop as the variety of means of communications available."[26] In fact, social media's value is so widely recognized that—in addition to being a regular topic of coaching and education in the Islamic State of Syria's (ISIS) publications—social media strategies for converting westerners are now codified in instruction manuals regularly utilized by organizations like Al-Qaeda and ISIS.[27]

Social media is best defined in terms of the characteristics that distin-

Support Claims, 37 LOY. L.A. ENT. L. REV. 1, 7 (2017) ("The increased presence of terrorist organizations on social media has generated a growing concern that groups like ISIS are increasingly using these communication sites in sophisticated ways.").

24. *See* Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53, 64 (2017). "As a result [of social media], 'foreign terrorist organizations now have direct access into the United States like never before.'" *Id.* (quoting *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, Hearing before the S. Comm. on the Judiciary*, 114th Cong. (2015) (statement of Sally Quillian Yates, Deputy Att'y Gen., Department of Justice and James B. Comey, Director, Federal Bureau of Investigation)).

> [Terrorists] use social networks to recruit, to inspire, and to connect, but they also rely on social media bystanders—everyday, regular people—to spread the impacts of their terror further than they could themselves, and to confuse authorities with misinformation. That amplification encourages more terrorism, inspires copycats, and turns the perpetrators into martyrs. It also traumatizes the families of the murdered victims, as well as the public at large.

Emily Dreyfuss, *Think Before You Tweet in the Wake of an Attack*, WIRED (May 23, 2017, 4:29 PM), https://www.wired.com/2017/05/think-tweet-wake-attack/.

25. Klein & Flinn, *supra* note 24, at 63. These findings are based upon a decade-long study of encoded and public internet sites utilized by terrorist organizations and their supporters. *Terrorist Groups Recruiting Through Social Media*, CBC NEWS (Jan. 10, 2012, 12:15 PM), http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social-media-1.1131053. The study also included monitoring of "video clips and snippets relating to global terrorism on various arenas such as Facebook, Twitter, chat rooms, YouTube and Myspace, among others." *Id.*

26. Klein & Flinn, *supra* note 24, at 64.

27. *See* Engel, *supra* note 10; Brian Fishman & Abdullah Warius, *A Jihadist's Course in the Art of Recruitment*, CTC SENTINEL (Feb. 2009), https://ctc.usma.edu/app/uploads/2010/06/Vol2Iss2-Art5.pdf; *see generally* Anthony F. Lemieux et al., Inspire *Magazine: A Critical Analysis of Its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model*, TERRORISM & POL. VIOLENCE (2014) (analyzing Al-Qaeda's English-language publication regarding the recruitment methods of terrorist organizations).

guish it from more traditional web media models.[28] Its "interactivity, reach, frequency, usability, immediacy, and permanency" make it unique and particularly suited to accomplishing the ends of terrorists.[29] Where more traditional media sources, even those published via online platforms, utilize a "one–to–many" model that focuses on disseminating the ideas of a few to a larger public, social media allows for mutual and equal engagement.[30] The average American spends at least two hours a day on their social media accounts, reading, posting, responding, and otherwise engaging in online communities.[31] This wide reach and interactive nature creates an ideal, target-rich environment for virtual terror activity.[32]

A. General Use of Social Media by Terrorists

Terror communications may be categorized in a variety of ways.[33] However, at a fundamental level, all terrorist use of social media platforms is intended to accomplish at least one of four purposes: (1) recruitment, (2) training, (3) action, or (4) public terror.[34]

---

28. *See generally* Weimann, *supra* note 21, at 2–3 (discussing what distinguishes social media from traditional media forums and forms).

29. *Id.* at 2.

30. *Id.*

31. Carolyn Sun, *How Do Your Social Media Habits Compare to the Average Person's?*, ENTREPRENEUR (Dec. 14, 2017), https://www.entrepreneur.com/slideshow/306136. For certain age groups, this number rises exponentially. *Id.* Teenagers, in particular, have an exponentially higher rate of usage, averaging nine hours a day. *Id.*; *see also Social Networking Reaches Nearly One in Four Around the World*, EMARKETER (June 18, 2013), https://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976 (explaining how social media has penetrated international markets and continues to grow rapidly). This heightened use among children and young adults is particularly concerning because they are precisely the demographic that terrorists are utilizing social media to target. *See* Harriet Taylor, *Most Young Terrorist Recruitment is Linked to Social Media, Said DOJ Official*, CAMBRIDGE CYBER SUMMIT (Oct. 5, 2016, 2:26 PM), https://www.cnbc.com/2016/10/05/most-young-terrorist-recruitment-is-linked-to-social-media-said-doj-official.html.

32. Weimann, *supra* note 21, at 3. The interactive form of social media is also appealing to terrorists because it allows for proactive engagement in recruiting and conversion, which distinguishes it from the sit-and-wait mentality necessitated by static websites or dedicated chatrooms. *Id.*; *see also infra* Section II.A.1.

33. *See, e.g.*, Klein & Flinn, *supra* note 24, at 64–65 (discussing these same activities in three categories); Weimann, *supra* note 21, at 3 (explaining that terrorists' primary online purposes are propaganda, radicalization, and recruitment).

34. *See generally* Gabriel Weimann, *How Modern Terrorism Uses the Internet*, Special Report, U.S. INST. PEACE (Mar. 2004), https://www.usip.org/sites/default/files/sr116.pdf (explaining the method and impact of internet use by terrorist organizations). "The mass media, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyberterrorism and paid

1. Recruitment

The advent of social media removed two major barriers that previously limited the ability of terrorists to use the internet for active recruiting.[35] First, it created space for proactivity by terror supporters,[36] and second, it largely negated the impact of geographical separation.[37] By necessity, traditional terrorist web forums required extremist recruiters to wait for a potential new recruit or convert to take the first step by actively seeking out a jihad site or forum.[38] Social media, in contrast, enables terrorist recruiters to make the first move, actively reaching out and initiating relationships with strategically targeted recruits.[39]

Terrorists approach social media much like pedophiles do.[40] Unrestricted use of social media sites leave children and teenagers uniquely vulnerable to anonymous "friends" with bad intentions, whether those intentions are to inspire children to participate in terrorist activity or to groom them for abuse by a pedophile.[41] Just like pedophiles, terrorists are drawn to online com-

insufficient attention to the more routine uses made of the Internet. Those uses are numerous and, from the terrorists' perspective, invaluable." *Id.* at 1. Terrorists use social media as a central tool in accomplishing many goals "ranging from psychological warfare and propaganda to highly instrumental uses such as fundraising, recruitment, data mining, and coordination of actions." *Id.*

35. *See infra* notes 36–37 and accompanying text; Weimann, *supra* note 21, at 14–15. The advent of social media reshaped the world of terrorism as a whole, opening up greater opportunities for Middle Eastern organizations to reach into the West and a greater understanding of how terrorists function as well as the goals they seek to achieve. Weimann, *supra* note 21, at 14–15. This insight must be capitalized upon to avoid allowing greater harm to result from the doors opened by social media. *Id.*

36. *See* Weimann, *supra* note 34, at 3–4.

37. Gabriel Weimann, *Terror on Facebook, Twitter, and YouTube*, 16 BROWN J. WORLD AFF. 45, 53 (2010) [hereinafter Weiman, *Terror*] ("Terrorist groups are no longer confined to specific regional boundaries—now terrorist networks can recruit and members [can be] located in any part of the globe. A person in the United States can literally take a terrorist training course within the privacy of their bedroom." (footnote omitted)).

38. Weimann, *supra* note 21, at 3.

39. *Id.* ("[S]ocial networking allows terrorists to reach out to their target audiences and virtually 'knock on their doors' . . . .").

40. *See, e.g.*, Anthony Faiola & Souad Mekhennet, '*What's Happening to Our Children?'*, WASH. POST (Feb. 11, 2017), http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely-the-islamic-state-thinks-theyll-make-perfect-terrorists/ (discussing how ISIS recruiters use a pedophile-like grooming process with young recruits).

41. *See 'Facebook' Terrorism Investigation*, ADVERTISER (Apr. 4, 2008, 6:00 AM), http://www.adelaidenow.com.au/news/facebook-terrorism-investigation/news-story/69a8ffd26505d472726348297a80f67f?sv=662b980c75ec55a62e7a84791e6e7e4a. As Shanton Change, a senior technology lecturer at Melbourne University, noted, "The issue with having friends on Facebook, whether you know them or not, is once they're your friend, they can access and have a look at any-

munities because these sites provide a target-rich environment, full of young and impressionable users who may be easily persuaded and manipulated.[42] Once terrorists locate a target, they continue to parallel the techniques employed by pedophiles.[43] They build trust, "deploying flattery and attention while pretending to be friends."[44] Daniel Koehler, director of the German Institute on Radicalization and Deradicalization Studies, describes the methods employed by these recruiters as part of a "structured recruitment process" that begins with casual conversation and ultimately culminates when the recruiters utilize their young recruits as disposable weapons.[45]

---

thing about you listed on there." *Id.* While young adults are particularly targeted and vulnerable, ISIS and similar organizations apply these same techniques in targeting recruits of all ages and backgrounds. *See generally* Lorenzo Vidino & Seamus Hughes, *ISIS in America: From Retweets to Raqqa*, PROGRAM ON EXTREMISM: GEO. WASH. U. (Dec. 2015), https://www.stratcomcoe.org/download/file/fid/2828.

42. Weimann, *supra* note 21, at 3.

> For lonely young people in transition, [terrorist groups] provide[] a quick fix to the perennial problems of human life. Vulnerable people don't tend to fact check when existential relief is easily and cheaply attained with little effort. Specifically, the relief in question concerns the human desire for identity, certainty, social connection, meaning, the optimal amount of freedom, and glory.

Omar Sultan Haque et al., *Why Are Young Westerners Drawn to Terrorist Organizations Like ISIS?*, PSYCHIATRIC TIMES (Sept. 10, 2015), http://www.psychiatrictimes.com/trauma-and-violence/why-are-young-westerners-drawn-terrorist-organizations-isis.

43. *See* Faiola & Mekhennet, *supra* note 40. Both terrorists and pedophiles employ a relationship building methodology that relies heavily upon flattery and relationship-building. *Id.* The internet enables terrorist agents to reach out to and cultivate relationships with individuals with particular vulnerabilities that make them susceptible to unwise actions. *See* J.M. Berger, *How Terrorists Recruit Online (And How to Stop It)*, BROOKINGS: MARKAZ (Nov. 9, 2015), https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/.

44. Faiola & Mekhennet, *supra* note 40. Terrorists and pedophiles also tend to target youths who are already considered "at-risk." *See id.*

> For instance, [a] 12-year-old detained in December after building his own bomb — which failed to go off only because of a faulty fuse — had been visited frequently by social workers because his father had a history of violence, according to German officials familiar with the case, who spoke on the condition of anonymity to discuss a juvenile. The son of Kurdish Iraqi immigrants, the boy had begun attending a local mosque — alone — that had been previously linked to an Islamist movement.

Id.

45. *Id.* Terrorists capitalize on the weaknesses of these young individuals, often utilizing their isolation and vulnerabilities against them. *See* Rukmini Callimachi, *ISIS and the Lonely American*, N.Y. TIMES (June 27, 2015), https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html. Their converts are often U.S. citizens and frequently those that would never be expected. *Id.* In 2015, the New York Times published an expose on the story of a young woman named Alex, a twenty-three-year-old American Sunday school teacher who converted to Islam after aggressive online recruitment by members of ISIS. *Id.* They attempted to convince her and her brother to run away to Syria. *Id.*

Abu Hurriya, a former Al-Qaeda member who was recruited as a teenager and later served as a "chief propagandist" for Al-Qaeda in the United States, analogized the methods employed by these groups to the process of gang recruitment.[46] Hurriya recognized that "ISIS recruitment video[s] with . . . panoramic views and warm camaraderie hit[] the sweet spot for angry young men and women who are searching for a purpose in life and a community of like-minded souls."[47] Still other experts draw a connection between social media recruitment by terrorist organizations and social media recruitment of sex trafficking victims.[48] Ultimately, whether a recruiter is looking to manipulate a target into bombing a subway, joining a gang, or trusting a pedophile or trafficker, social media offers the same advantages in helping to accomplish their criminal ends: an ideal method for finding and reaching their ideal targets while they sit "safely" in their own homes.[49]

In the United States, the rise of social media has also particularly benefited ISIS and other international terrorist organizations by removing the geographical barrier once provided by an ocean and thousands of miles.[50] "The global community created by social networks and interactive forums on the internet is advancing cultural awareness and reconciliation efforts, but it is also advancing terrorists' goals to share their extremist messages to

46. Elizabeth Cohen & Debra Goldschmidt, *Ex-Terrorist Explains How to Fight ISIS Online*, CNN (Dec. 21, 2015, 11:24 AM), https://www.cnn.com/2015/12/18/health/al-quaeda-recruiter-fight-isis-online/index.html. Hurriya's name has been changed for his own safety. *Id.*

47. *Id.* Hurriya also analogized the reasoning for the appeal of such groups to teenagers to that of gang recruitment. *Id.* These are lost "seekers" looking for a place to belong—and groups like ISIS and Al-Qaeda offer that belonging. *Id.*

48. *See* Alan Rozenshtein, *It's the Beginning of the End of the Internet's Legal Immunity*, FOREIGN POL'Y (Nov. 13, 2017, 9:44 AM), http://foreignpolicy.com/2017/11/13/its-the-beginning-of-the-end-of-the-internets-legal-immunity/ (discussing how terrorism and trafficking actions against social media companies face similar challenges).

49. See *supra* text accompanying notes 38–48 for discussion of the methodology employed by recruiters in all these contexts. "[S]ocial media channel[s] inspire[] serious research that goes thousands of words deeper to address the biggest issues of our day: extremism, jihad, gangs, misinformation, and, of course, how to become the next famous influencer." Michael Martinez & Lori Cameron, *Twitter: How Social Media Intersects with Influence, Jihad, Gangs, Drugs*, INTELLIGENT SYSTEMS (Oct. 13, 2017), https://publications.computer.org/intelligent-systems/2017/10/13/twitter-research-influence-maximization-jihad-gangs-drugs/.

50. Weimann, *Terror*, *supra* note 37. The ease with which ISIS now recruits here in the United States is staggering and concerning. Daniel Byman, *Beyond Iraq and Syria: ISIS' Ability to Conduct Attacks Abroad*, BROOKINGS (June 8, 2017), https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/. Such recruitment creates a significant threat to U.S. security, particularly as research shows that sixty percent of ISIS recruits who consider travelling to fight in the Middle East do not end up travelling, but eventually become involved in a terrorist plot. *Id.*

global audiences."[51] Major terror organizations today play the role of media conglomerates in addition to murderers.[52] They produce recruitment videos that rival Hollywood productions in their quality and presentation, while simultaneously glorifying the killing of their enemies and hallowing the supposed beauty of their own community and social hierarchy.[53]

Over the past few years, the predominant terror threat within the United States has come at the hands of lone-wolf attackers.[54] Historically speaking, lone-wolf attacks came at the hands of social outsiders.[55] They were individuals like Ted Kaczynski, the infamous "uni-bomber" who was later diagnosed as a paranoid schizophrenic.[56] Experts historically considered this type of mental illness, coupled with incoherent and individualistic ideological beliefs, definitive traits of lone-wolf actors.[57] Today, however, the label

51. Weimann, *Terror*, *supra* note 37, at 53.

52. Koerner, *supra* note 9. Terrorist recruiters on social media gain a celebrity status for their work. *Id.* Their converts and fellow caliphate members look to them for leadership and guidance. *Id.*

53. Easterly & Geltzer, *supra* note 8. "This is largely how the Islamic State has been able to penetrate our borders: not through flows of refugees intent on conducting attacks against Americans but through the bits and bytes of today's digital age." *Id.*; *see* Simon Parkin, *How Isis Hijacked Pop Culture, From Hollywood to Video Games*, GUARDIAN (Jan. 29, 2016, 11:33 AM), https://www.theguardian.com/world/2016/jan/29/how-isis-hijacked-pop-culture-from-hollywood-to-video-games. Films released by terrorist groups today "employ[] the aesthetic of contemporary Hollywood films, video games and TV shows, with their tracks and zooms, their whizzing motion graphics, their slow-mo gunfire and rhythmic edits." *Id.* They utilize these films to idealize a life of making "playful violence of action movies, sports and video games earnest." *Id.*; *see also British Jihadi Compares Syria War to Call of Duty*, BBC (June 13, 2014), http://www.bbc.co.uk/newsbeat/article/27838978/british-jihadi-compares-syria-war-to-call-of-duty (sharing the story of a British ISIS recruit who now describes his life with ISIS as "better than that game Call of Duty").

54. *See* Weimann, *supra* note 21, at 14 ("Lone wolf terrorism is the fastest-growing kind of terrorism, especially in the West, where all recent lone wolf attacks involved individuals who were radicalized, recruited, trained, and even launched on social media platforms."). Lone-wolves today are very different from those of previous eras in that, even when they are entirely independent actors, they usually have ideological motivations, whereas predecessor lone-wolves often executed their attacks from motivations tied to diagnosable conditions. Tom Mockaitis, *The Changing Face of Lone Wolf Terrorism*, HUFFINGTON POST (Nov. 1, 2017 12:53 PM), https://www.huffingtonpost.com/entry/the-changing-face-of-lone-wolf-terrorism_us_59f9f9b2e4b0b7f0915f636c.

55. *See* Mockaitis, *supra* note 54. These individuals often suffered from diagnosable mental illness and were motivated by fantastical ideologies or illusions. *Id.*

56. *Id.* Another example of a "classic" lone-wolf is Anders Breivik, a Norwegian who killed seventy people in 2011 between a bombing in Oslo and an attack on a youth camp. *Id.*

57. Emily Corner et al., *Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence*, 39 STUD. CONFLICT & TERRORISM 560, 560 (2016) ("[R]esearch on the link between mental health problems and terrorist activity has had a . . . well-documented history. Early studies highlighted very specific mental disorders like psychopathy or personality disorders such as narcissism.") (footnotes omitted); *see, e.g.*, H.H.A. Cooper, *Psychopath*

"lone-wolf terrorist," which is given to terrorist actors who lack of membership in formal terror organizations, is a misleading misnomer.[58] Modern lone-wolves are not alone at all. Rather, they are the product of social media recruitment. They have an entire virtual, global community behind them, recruiting them, supporting them, and pushing them toward radicalization and action.[59] They identify with an established ideology and are motivated by those beliefs.[60] In the end, lone-wolves act alone, but they would never act at all without the urging and manipulation of their online "friends."[61]

2. Training

It is not just the increased opportunity for proactivity in recruitment that makes social media so dangerous.[62] Terrorist actors have perfected the art of using social media to not only target new recruits but to train, educate, weaponize, and mobilize them without fear or risk of consequence.[63] The British Security Service, MI5, characterizes this use of the internet as conducting a "virtual training camp."[64] This virtual training provides the oppor-

as Terrorist, 2 LEGAL MED. Q. 253, 256 (1978) (comparing psychopathic qualities and characteristics with behaviors of terrorists).

58. *See* Weimann, *supra* note 21, at 14; *see also* Gabriel Weimann, *Virtual Packs of Lone Wolves*, MEDIUM (Feb. 25, 2014), https://medium.com/its-a-medium-world/virtual-packs-of-lone-wolves-17b12f8c455a [hereinafter Weimann, *Virtual Packs*] (describing the growth of lone-wolf terrorism).

59. *See* Weimann, *supra* note 21, at 13. All recent lone-wolf attackers were at least partially radicalized on social media sites. *Id.*

60. *See generally* Chris Strohm, *What's Behind the Rising Threat of Lone-Wolf Terror*: *Quick-Take*, WASH. POST (Dec. 11, 2017), https://www.washingtonpost.com/business/whats-behind-the-rising-threat-of-lone-wolf-terror-quicktake/2017/12/11/fefae6c4-dea6-11e7-b2e9-8c636f076c76_story.html (discussing the rise of the new lone-wolf).

61. Easterly & Geltzer, *supra* note 8. "[T]he Islamic State has . . . explicitly encouraged its recruits to be opportunistic: to attack where they are, when they can, with what they have." *Id.* The leadership provides broad tactical and strategic direction, but it is ultimately individuals—lone-wolves—who "specifically conceive[]" and implement these plans. *Id.*

62. *See infra* notes 63–75 and accompanying text. The danger created by social media's use as a recruitment mechanism is amplified by the platform it provides for ongoing indoctrination and practical training. *See infra* notes 63–75 and accompanying text.

63. *See* Gabriel Weimann, *Terrorist Migration to Social Media*, 16 GEO. J. INT'L AFF. 180, 183 (2015) [hereinafter Weimann, *Terrorist Migration*] ("Online radicalization is a multistep process, which requires a gradual transition and numerous phases . . . .").

64. *Terrorist Training and Indoctrination,* SECURITY SERV. MI5, https://www.mi5.gov.uk/terrorist-training-and-indoctrination (last visited Sept. 28, 2018) ("Extremists use . . . social media to recruit and radicalise individuals through videos and propaganda . . . . [S]ocial media messages can also provide advice and instructions on how to plan and prepare for attacks, acting as a 'virtual training camp' or ideas forum.").

tunity for individuals to be further radicalized and trained in both doctrinal and practical matters.[65] For instance, Dzhokhar and Tamerlan Tsarnaev, the bombers in the 2013 Boston Marathon bombing, actually learned how to make the bombs they used in their attacks via Al-Qaeda's online magazine, *Inspire*.[66]

After capitalizing on social alienation and frustration to build initial rapport and virtual relationships with potential converts, recruiters turn their attention from preliminary conversion to in-depth indoctrination.[67] Developing deeper relationships enables these actors to pinpoint members who possess particular proclivities and then to capitalize on them, encouraging their trusting recruits toward self-radicalization and, eventually, acts of radical violence against others.[68] Recruiters provide new converts with educational tools, equipping the attackers to build their weapons and assist in strategic decision-making.[69] They use social media to equip their recruits with the means and opportunity to complete their own attacks, functionally providing a virtual support team.[70]

This transition toward increasingly radical, action-based content goes hand-in-hand with a movement from "public, open source communications such as [public] Facebook and Twitter posts to private communications, such as encrypted messaging, . . . [a transition] referred to as 'going dark.'"[71]

---

65. Weimann, *Virtual Packs*, *supra* note 58. Numerous terror attacks conducted in the United States in recent years have been similarly linked to *Inspire's* radical content and specific training materials. *Id.*

66. *Boston Marathon Terror Attack Fast Facts*, CNN (Mar. 25, 2018, 6:42 PM), https://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts/index.html. The Boston bombing occurred on April 15, 2013. *Id.* The Tsarnaevs set off two bombs near the finish line of the Boston Marathon. *Id.* They "killed three people and injured at least 264" more. *Id.*

67. Weimann, *Terrorist Migration*, *supra* note 63, at 184. Recruiters at this stage transition to more intimate and in-depth relationship building, emphasizing "religious, political, or ideological material." *Id.*

68. *Id*.

69. *See, e.g.*, Domonoske, *supra* note 1.

70. Dep't of Homeland Sec., *Terrorist Use of Social Networking Sites Facebook Case Study*, PUB. INTELLIGENCE (Dec. 5, 2010), http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study. Social media provides individualized relational and tactical support as well as technical training, like bomb-building plans. *Id.*

71. Klein & Flinn, *supra* note 24, at 67. "[Terrorists] make jihad look fun, exciting, and attractive to an online audience." Mike Rogers, *How ISIS Uses the Internet to Recruit New Members (Hint: It Involves Kittens)*, N.Y. DAILY NEWS (Sept. 6, 2017, 11:07 AM), http://www.nydailynews.com/news/national/isis-internet-recruit-members-hint-kittens-article-1.3473890#. As Humera Khan, executive director of a think tank focused on fighting Islamic extremism, noted, "[ISIS]'s message is sexy." David Talbot, *Fighting ISIS Online*, MIT TECH. REV. (Sept. 30, 2015), https://www.technologyreview.com/s/541801/fighting-isis-online/.

"Going dark" provides the context and space for this more in-depth training.[72] The end-to-end encryption provided by Facebook messenger and similar applications provides an added layer of protection for recruiters and opens the door for more direct conversation.[73] Instead of broadly providing general recruitment literature and posting catchy YouTube clips, the recruiter turns these one-on-one conversations toward topics like explosive construction, weapons acquisition, the beauty of martyrdom, and what it means to "join the jihad."[74] The tone of the entire interaction turns from conversion and inclusion to commitment and sacrifice.[75] This paves the way for the ultimate harm.[76]

3. Action

Increasingly, terrorist groups are recognizing "electronic jihad" as divine and honorable in and of itself.[77] This status, in turn, helps to draw more western recruits and incites the creation of more recruiters.[78] Posts on leading jihadist forums encourage followers to do jihad electronically, promising followers that those who engage in this form of jihad are as invaluable—and will be as rewarded, just as those risking injury or death in physical attacks.[79] However, the *impact* and endgame of electronic jihad are not con-

72. *See, e.g.*, Callimachi, *supra* note 45 (explaining how members of the Islamic State educate potential converts via skype and similar platforms).

73. Jasper Hamill, *How Terrorists Use Encrypted Messaging Apps to Plot, Recruit, and Attack*, N.Y. POST (Mar. 28, 2017, 12:10 PM), https://nypost.com/2017/03/28/how-terrorists-use-encrypted-messaging-apps-to-plot-recruit-and-attack/. These applications allow "extremists to spread terror across the world like never before." *Id.*

74. *See* Berger, *supra* note 43. The shift to private communication is followed by a conversational shift. *Id.* The terror supporters now begin to "probe to figure out what the target is most likely to do (usually travel to join ISIS, or carry out terrorist attacks at home), then encourage the target to take action." *Id.*

75. See *infra* Section II.A.3 for a discussion of the next phase of conversion and the dangerous impact jihadi created on the internet.

76. *See infra* Section II.A.3.

77. George Leopold, *Report: Electronic Jihad Grows in Sophistication*, DEF. SYS. (July 1, 2016), https://defensesystems.com/articles/2016/07/01/isis-electronic-jihad-on-rise.aspx. "Electronic jihad" encompasses a range of behavior, including recruitment and radicalization, while also extending to more traditional acts of hacking and cyber terrorism. *See id.*

78. *See* Weimann, *supra* note 21, at 3–4. According to a prominent jihadist scholars, electronic jihad plays a significant role in the Islamic faith and those who choose to engage in such online terrorism will receive the divine status of "mujaheed." *Id.*; *see also, e.g.*, Callimachi, *supra* note 45 (acknowledging the appeal of the tightknit and dedicated online community of terrorist organizations).

79. *See* Weimann, *supra* note 21, at 3–4. This is not universally accepted but appears to be gain-

fined to cyberspace.[80] In some cases, online initiation and education leads these individuals to cross the world to physically join ISIS, Al-Qaeda, or other jihadist groups in the Middle East.[81] More than 40,000 fighters from 110 countries have left their homes to fight for ISIS, and more have tried.[82] One such willing recruit was Jaelyn Delshaun Young (Young) from Vicksburg, Mississippi.[83] A former cheerleader and honors student, she sent online messages to individuals she believed to be ISIS members stating that she could not "wait to get to Dawlah [ISIS territory]" so she could "be amongst [her] brothers and sisters."[84]

In cases like Young's, private communication becomes the gateway to coordination enabling the actualization of such plans.[85] For others, increas-

ing support among jihad supporters. *Id.* at 4. In addition to jihad in the form of internet propagandizing and recruiting, Europe and the United States are increasingly concerned with the possibility of impending cyber-attacks, which are encouraged as part of the electronic jihad. *See generally* Edwin Mora, *House Task Force: Al-Qaeda 'Probed' U.S. Infrastructure to Launch Cyber Jihad*, BREIT BART (Dec. 22, 2016), http://www.breitbart.com/national-security/2016/12/22/house-task-force-al-qaeda-probed-u-s-infrastructure-launch-cyber-jihad/ ("Al-Qaeda has explored the critical infrastructure in the U.S. . . . in search of vulnerabilities to carry out 'electronic jihad.'").

80. *See* Aryn Baker, *How ISIS Is Recruiting Women from Around the World*, TIME (Sept. 6, 2014), http://time.com/3276567/how-isis-is-recruiting-women-from-around-the-world/. Westerners from across the United States and Europe have migrated to Syria in order to join jihadist groups after building relationships with recruiters via social media. *Id.* Women in particular have become the target of this style of recruiting. *Id.* Deceived and enticed via social media, these women go to start a new life, often not expecting the oppressive, segregated lifestyle still faithfully observed by those in the jihad community. *Id.*

81. *See generally* Lisa Blaker, *The Islamic State's Use of Online Social Media,* 1 MIL. CYBER AFF. 1, 6–7 (2015) (discussing how social media is used to spur western converts to migration).

82. Hollie McKay, *Almost All American ISIS Fighters Are Unaccounted for*, N.Y. POST (Oct. 27, 2017), https://nypost.com/2017/10/27/almost-all-american-isis-fighters-are-unaccounted-for/. Approximately 300 of these are Americans. *Id.*

83. *See* Paul Sperry, *Meet the American Women Who are Flocking to Join ISIS*, N.Y. POST (May 13, 2017, 9:34 PM), https://nypost.com/2017/05/13/meet-the-western-women-who-are-flocking-to-join-isis/.

84. *Id.* Young sent these messages to undercover FBI agents. *Id.* She was subsequently arrested and is currently serving a twelve-year sentence for conspiring to provide material support to ISIS. *Id.*

85. *See, e.g.*, Sara Khan, *The Jihadi Girls Who Went to Syria Weren't Just Radicalised by Isis—They Were Groomed*, INDEP. (Feb. 25, 2015, 12:52 PM), http://www.independent.co.uk/voices/comment/the-jihadi-girls-who-went-to-syria-werent-just-radicalised-by-isis-they-were-groomed-10069109.html ("Using extremist theology and social media, they target young girls with the hope of persuading them to help build their so-called 'state.'"); *see also* Richard Engel et al., *The Americans: 15 Who Left the United States to Join ISIS*, NBC NEWS (May 16, 2016, 7:13 PM), https://www.nbcnews.com/storyline/isis-uncovered/americans-15-who-left-united-states-join-isis-n573611 (tracing the stories of American recruits to ISIS, including many whose conversion involved internet use).

ing radicalization does not lead to an international transplant.[86] Rather, it leads them to take action closer to home, and this reality has been the single greatest factor contributing to the uptick in domestic lone-wolf terror attacks over the past decade and a half.[87] Especially over the past few years—as European and American governments prioritized making it more difficult for recruits to defect to Syria and nearby nations—recruiters have begun encouraging would-be martyrs to stop wasting their efforts and energy in attempts to reach the Islamic State and instead start attacking where they are.[88] As ISIS continues to lose ground in the Middle East, the group and its affiliates have continued to push for more international attacks—and again, it is social media that has played a key role in encouraging and enabling these attacks.[89] For example, in the past few years, ISIS has particularly urged lone-wolves to conduct vehicular-based attacks; social media is part of what enables ISIS to make such pushes.[90] In November 2016, ISIS posted on Twitter and Facebook, praising the "deadly and destructive capability of the motor vehicle" and offering ideas for conducting such attacks.[91] A month

86. *See* Lorenzo Vidino, *7 Things You Need to Know About Jihadists in the United States*, POLITICO MAG. (June 15, 2016), https://www.politico.com/magazine/story/2016/06/things-you-need-to-know-about-jihadists-terrorists-extremists-the-united-states-213964 ("Here in the U.S., people who embrace the ideology stay in the country . . . . In the U.S., jihadists also have easy access to automatic weapons, and they decide to carry out their attacks domestically—in San Bernardino, Chattanooga, Orlando. This is why America has seen quite a high number of domestic attacks compared with European countries.").

87. See *supra* Section II.A.1 for a discussion of online recruitment and the creation of lone-wolf terrorists; *see also* Byman, *supra* note 7 (tracing the evolution of lone-wolf terrorism in the United States).

88. *See* Rukmini Callimachi, *Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots from Afar*, N.Y. TIMES (Feb. 4, 2017), https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html (quoting an Islamic State spokesman as saying, "If the tyrants have closed in your faces the door of hijrah, [the journey home to the Islamic State], then open in their face the door of jihad.").

89. *See* Zach Beauchamp, *ISIS's Defeat in Iraq and Syria Makes Attacks Like in New York Inevitable*, VOX (Dec. 11, 2017, 11:23 AM), https://www.vox.com/world/2017/11/1/16591458/new-york-attack-isis-islamic-state-strategy.

90. Greg Myre, *As ISIS Promotes Vehicle Attacks, Terrorists Strike in Europe and U.S.*, NPR (Nov. 1, 2017, 12:35 PM), https://www.npr.org/sections/thetwo-way/2017/11/01/561327621/as-isis-promotes-vehicle-attacks-terrorists-strike-in-europe-and-u-s. "ISIS began aggressively promoting vehicle attacks [in 2016] with detailed instructions . . . ." *Id.*

91. Andrew O'Reilly, *ISIS Social Media Accounts Promoted Use of Trucks as Weapons More Than a Month Before Berlin Attack*, FOX NEWS (Dec. 20, 2016), http://www.foxnews.com/world/2016/12/20/isis-social-media-accounts-promoted-use-trucks-as-weapons-more-than-month-before-berlin-attack.html. The posts were made in conjunction with the publication of an online article in the radical magazine, *Rumilyah*, or Rome. *Id.* The article describes the impact of such attacks with chilling specificity:

later, there was a vehicular attack in Berlin.[92] This became the first in a long succession of vehicular attacks over the subsequent year and a half.[93]

In numerous other cases, attackers have used social media as a means of declaring their allegiances prior to conducting an attack or as a platform for explaining the motivation for their attack.[94] Some use social media platforms to communicate with their supporters in order to receive the encouragement they need to "go through with it."[95] Still others, like Omar Mateen, the now-infamous shooter from the Orlando Pulse nightclub attack, employ social media in their actual attack.[96] In the aftermath of that attack, Florida Senator Ron Johnson reached out to Mark Zuckerberg, Facebook's founder, when Johnson's staff discovered that Mateen used social media before and during the attack to research and post terror-related content.[97] Johnson urged, as many others have since, that when a social media company plays this significant of a role in an attack, the site becomes an ally in the fight against terrorism, rather than simply a facilitating bystander of it.[98]

> The method of such an attack is that a vehicle is plunged at a high speed into a large congregation of kuffar (an Arabic term for "unbeliever"), smashing their bodies with the vehicle's strong outer frame, while advancing forward—crushing their heads, torsos, and limbs under the vehicle's wheels and chassis—and leaving behind a trail of carnage.

Id.

92. Darran Simon, Ralph Ellis, & Frederik Pleitgen, *Berlin Christmas Market: 12 Dead, 48 Hospitalized in Truck Crash*, CNN (Dec. 19, 2016, 9:52 PM), https://www.cnn.com/2016/12/19/europe/berlin-christmas-market-truck/index.html. On December 19, 2016, a tractor trailer drove full-speed into a crowded Christmas market. *Id.* Twelve people were killed, and forty-eight others were hospitalized. *Id.*

93. *See* Myre, *supra* note 90.

94. *See, e.g.*, Greg Myre, *A Mass Shooter 'Pledges Allegiance' to ISIS. What Does This Mean?*, NPR (June 13, 2016, 4:32 PM), https://www.npr.org/sections/parallels/2016/06/13/481284054/a-mass-shooter-pledges-allegiance-to-isis-what-does-this-mean ("Tashfeen Malik declared her allegiance to ISIS in a Facebook post last December as she and her husband launched a shooting spree that left 14 dead in San Bernardino . . . .").

95. See *supra* notes 62–84 and accompanying text for a discussion of how recruiters and trainers encourage virtual recruits to take physical action.

96. Malia Zimmerman, *Orlando Terrorist's Chilling Facebook Post from Inside Club Revealed*, FOX NEWS (June 16, 2016), http://www.foxnews.com/us/2016/06/15/orlando-terrorists-chilling-facebook-posts-from-inside-club-revealed.html.

97. *Letter from Sen. Ron Johnson to Facebook Regarding Orlando Shooter's Posts*, FOX NEWS (June 15, 2016), http://www.foxnews.com/us/2016/06/15/letter-from-sen-ron-johnson-to-facebook-regarding-orlando-shooters-posts.html.

98. *Id.*

4. Public Terror

The damaging impact of social media does not end with the execution of an attack.[99] A trademark of modern terrorism is its unapologetic brutality, and social media provides a means to exponentially magnify and glorify that.[100] Terrorists have utilized social media to great effect to not only communicate and create actual attacks but to inspire terror among innocent individuals, even those who are thousands of miles away from any attack taking place.[101] As early as 2004, Al-Qaeda leadership began utilizing YouTube and other online forums to publish videos specifically intended to inspire fear in the public, while simultaneously attracting those with sadistic proclivities as new recruits.[102] Today, when radical organizations make a political or military move, the way they frame it on social media can play a role every bit as significant as the organization's physical actions.[103] Researchers describe today's terrorist organizations, like ISIS, as having a signature "brand" in the same way as major companies like Nike and Coca-Cola.[104] Indeed, with the advent of social media, the brand of these organizations is, in many ways, more influential than physical control over land will ever be.[105] As Emily Dreyfuss, a senior editor for *Wired* magazine, explained it,

99. *See infra* notes 105–07 and accompanying text.

100. *See* Koerner, *supra* note 9 ("The Islamic State has long taken pride in its flair for developing content that is innovative and repugnant in equal measure.").

101. *See* discussion *supra* Section II.A.4.

102. Koerner, *supra* note 9. In 2004, Al-Qaeda published a video featuring the beheading of Nick Berg—a video that went viral in its own right. *Id.* Radical organizations use these types of videos to "recruit from the extremist fringe that gets excited by such cruel behavior." *Id.*

103. Emerson T. Brooking & P.W. Singer, *War Goes Viral*, ATLANTIC (Nov. 2016), https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/ ("[S]trip away the religious claims and the on-camera killings, and the ISIS online playbook looks much like any of the dozens of social-media-marketing 'how-to's circulated by consultants. The principles that have guided the Islamic State's viral success are the same ones used to publicize a new Taylor Swift album or the latest Star Wars movie.").

104. *See* Patrick Hanlon, *ISIS As Brand Movement*, MEDIUM (Feb. 11, 2015), https://medium.com/@hanlonpatrick/isis-as-brand-movement-e1637c7e3f62. "ISIS has a black flag, and a symbolic logo. They also wear distinctive clothing (including black masks). Weapons like RPGs and the AK47 distinguish and differentiate them. Other brands have icons, too. We rally around the American flag and logos for Nike, UnderArmour, Gatorade and other brands." *Id.*

105. *See* Jacob Olidort, *Brand Control is More Important to ISIS Than Territory*, WASH. INST. (Oct. 21, 2016), http://www.washingtoninstitute.org/policy-analysis/view/brand-control-is-more-important-to-isis-than-territory ("The group's pioneering use of jihadist social media and communications ensures that its message will continue resonating well past the loss of Mosul and other strongholds.").

> The potential harm that is done [by social media] is that it amplifies the goal of terrorism, which is not merely to maim or murder people but to actually incite fear at large. And so when you retweet gory images, one thing that you are doing is spreading fear from a small group . . . to the entire world. And that is the exact goal.[106]

This amplification of terror is an intentional choice specifically targeted to increase public fear and hysteria while, as a natural byproduct, opening the door for new recruits.[107]

B. Understanding the Key Social Media Actors

One of the dynamics that makes understanding the relationship between social media and terrorism so challenging is social media's inherently evolutionary nature.[108] Today, the primary actors in the social media world are websites and apps, including most predominantly Facebook, Twitter, YouTube, and Instagram.[109] These will undoubtedly shift; however, the underlying challenges and dangers these platforms present in the realm of modern terrorism will continue until something greater is changed.[110]

As Professor Marie-Helen Maras of the City University of New York explained, "Terrorism is a form of theater, each act of a terrorist, supporter, or follower is designed to provoke emotions in the audience to elicit a desired response from them."[111] Different social media platforms provide different "stages" on which terrorist actors may play out their dramas, and accordingly, these platforms can be used for different purposes.[112] Twitter's micro-blogging framework, for instance, provides the perfect setting for propaganda dissemination, while its messaging capabilities offer an ideal

106. Audie Cornish, *After a Terrorist Attack, Social Media Can Cause More Harm Than Good*, NPR (May 26, 2017, 5:44 PM), https://www.npr.org/2017/05/26/530257519/after-a-terrorist-attack-social-media-can-cause-more-harm-than-good.

107. *See id.*

108. *See generally* Weimann, *supra* note 21, at 15 (acknowledging that social media is constantly changing). This evolutionary element is also significant in that it increases the importance of taking a proactive approach to guarding against social media abuse by terrorists. *See infra* Parts IV–V for a discussion of why this is important and how the current laws permit this to occur.

109. Weimann, *supra* note 21, at 4, 8, 10.

110. See *supra* Part II for a discussion of how terrorists use social media.

111. Marie-Helen Maras, *Social Media Platforms: Targeting the "Found Space" of Terrorists*, 21 J. INTERNET L. 3, 4 (2017).

112. *See* Weimann, *supra* note 21, at 4–10 (discussing forms terrorism takes on major social networking sites).

setting for more in-depth indoctrination.[113] In contrast, Facebook's form lends itself to more diverse purposes.[114] Its multi-functionality, numerous features, and flexible form make it the ideal platform for everything from general reconnaissance and recruit targeting to providing recruits with tactical weapon training.[115] Meanwhile, YouTube's video-based structure limits its purposes, but its visual nature makes it inherently memorable and effective to both inspire potential recruits and instill crippling fear in potential victims.[116]

III. IMPOSING CIVIL MATERIAL SUPPORT LIABILITY UNDER THE ANTI-TERRORISM ACT AND ITS PROGENY

To be clear, none of these platforms would claim to be affirmative supporters of terrorism, and most do have some sort of formal protocol in place for addressing terror-related activity brought to their attention.[117] However, this does not stop terrorists from freely utilizing these sites, nor does it negate the significant cost of human life resulting from the failure of social media companies to adequately address the terrorist problem.[118] Congress has broadly recognized that the terrorists who pull triggers and hit detonators are not the only ones who bear responsibility for their actions.[119] It is well-

113. *Id.* at 5.

114. *See* Dep't of Homeland Sec., *supra* note 70. A study by the Department of Homeland Security found that terrorists use Facebook to: (i) share operational and tactical information; (ii) provide links and facilitate access to external radical content and discussion forums; (iii) serve as a media outlet for propaganda and extremist ideological messaging; and (iv) enable long-distance reconnaissance. *Id.*

115. Weimann, *supra* note 21, at 8.

116. *Id.* at 11.

117. *See* Michelle Malkin, *Twitter Just Deserted the Fight to Prevent Terror Attacks*, N.Y. POST (May 11, 2016), https://nypost.com/2016/05/11/twitter-just-deserted-the-fight-to-prevent-terror-attacks/. Historically, Twitter has been the most recalcitrant of these sites, although it is making renewed efforts. *Id.*; *see* Kerry Flynn, *Twitter's Crackdown on Terrorism Appears to Be Working*, MASHABLE (Sept. 19, 2017), https://mashable.com/2017/09/19/twitter-terrorism-data-transparency-report/#Q2Z3ss_nAmqq.

118. Tsesis, *supra* note 11, at 69. "While social media companies have independently worked to eliminate many terrorist postings, they are too often recalcitrant, tardy, or uncooperative in responding to law enforcement agencies' or public watchdogs' requests for removal of designated terrorists' web postings." *Id.* Although many are increasing their efforts under external pressure, these companies have repeatedly failed to take a proactive rule—or even to live up to the self-asserted rules established under their volunteer conduct codes. Liat Clark, *Twitter's Spam Tools Helped Shut Down 376,890 Terrorist Accounts in 6 Months*, WIRED (Mar. 21, 2017), http://www.wired.co.uk/article/twitter-transparency-report-2017.

119. *See* Jason Burke, *The Myth of the 'Lone Wolf' Terrorist*, GUARDIAN (Mar. 30, 2017),

established, as a fundamental principle of conspiracy in criminal law and specifically in the context of terrorism, that the one who makes it possible for someone else to pull a trigger bears just as much responsibility as that trigger-man.[120] This was the reasoning underlying the Anti-Terrorism Act of 1990's (ATA) material support provision.[121]

A. History and Purpose of Material Support and Secondary Liability Under the ATA

Congress created the original ATA as a response to two terrorist attacks that occurred during the mid-1980s.[122] The first involved the hijacking of a cruise ship, the Achille Lauro, by members of the Palestinian Liberty Organization (PLO).[123] Then, in 1988, the bombing of Pan American Flight 103 by Libyan terrorists led to the death of 270 people from twenty-one countries.[124] In the aftermath of those incidents, family members and survivors who attempted to bring suit against the individual terrorists and larger terror organizations responsible for their loss and suffering found that jurisdictional challenges under then-existing laws made it incredibly difficult for victims to effectively bring a cause of action for acts of terror that occurred primarily overseas.[125] One of the initial purposes of the ATA focused on re-

https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist.

120. *See, e.g.*, 18 U.S.C. §§ 2339A–2339B (2012) (outlining liability for providing material support to terrorists).

121. *See infra* Section III.A.

122. *See infra* notes 124–25; 18 U.S.C. § 2333 (2012).

123. Geoffrey Sant, *So Banks Are Terrorists Now?: The Misuse of the Civil Suit Provision of the Anti-Terrorism Act*, 45 ARIZ. ST. L.J. 533, 540 (2013). PLO-affiliated terrorists captured the Achille Lauro on October 7, 1985. *Id.* The terrorists murdered an elderly, wheel-chair bound passenger on board named Leon Klinghoffer and threw his body overboard. *Id.* His family and other passengers brought suit against the PLO, but they quickly encountered jurisdictional challenges because no law provided jurisdiction for prosecuting international terrorists under U.S. law. *Id.* at 540–41; *see* Klinghoffer v. S.N.C. Achille Lauro Ed Altri-Gestione Motonave Achille Lauro in Amministrazione Straordinaria, 937 F.2d 44, 50–52 (2d Cir. 1991).

124. *Terrorist Bombing of Pan Am Flight 103*, CIA (Nov. 21, 2012 8:28 AM), https://www.cia.gov/about-cia/cia-museum/experience-the-collection/text-version/stories/terrorist-bombing-of-pan-am-flight-103.html. In the second incident, Libyan terrorists hijacked and crashed Pan American Flight 103. Sant, *supra* note 123, at 544. The families wanted to sue the perpetrators. *Id.* at 543–44. However, due to jurisdictional challenges, attorneys did not even want to bring the suit. *Id.*

125. *See Anti-Terrorism Act of 1990* (C-SPAN television broadcast July 25, 1990) ("[V]ictims who have attempted to sue terrorists have encountered numerous jurisdictional hurdles and have found the courts reluctant to intrude in the absence of clear statutory mandate showing them what their jurisdictional boundaries are.").

solving this jurisdictional issue by creating causes of action specifically tailored to scenarios involving both domestic and international terrorism.[126] In particular, § 2333 created a civil cause of action for victims against those who commit international acts of terrorism.[127] However, in the years since, § 2333, and the ATA in general, have found their application in an increasing array of contexts, including litigation against third-party sponsors of terror and material supporters of terrorism.[128] Subsequent statutory developments helped to extend and create new grounds for these actions and define what constitutes an act of international terrorism.[129]

Four years after passing the original ATA provisions, Congress added supplemental provisions in § 2339 to criminalize the provision of material support to terrorists in any form.[130] Congress enacted these provisions in response to additional terror attacks in the 1990s.[131] Congress intended the material support provisions to be, "in effect[,] extremely expansive attempt

126. Sant, *supra* note 123, at 543–45.

127. 18 U.S.C. § 2333(a) ("Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees."). Despite the circumstances that spurred its creation, the provision actually lay dormant for over a decade after its passage. *See* Boim v. Quranic Literacy Inst. & Holy Land Found. for Relief & Dev., 291 F.3d 1000, 1001 (7th Cir. 2002) (noting the court's analysis of § 2333 was an issue of first impression); Sant, *supra* note 123, at 537.

128. Sant, *supra* note 123, at 555 ("Courts, sympathetic to victims of tragic acts of terrorism, appear to have creatively interpreted the ATA so as to allow these victims to pursue civil suits against third parties.").

129. Jack L. Goldsmith & Ryan Goodman, *U.S. Civil Litigation and International Terrorism*, *in* CIVIL LITIGATION AGAINST TERRORISM 109, 121–22 (John Norton Moore ed., 2004).

130. *See* 18 U.S.C. §§ 2339A–2339B. The material support criminalized by these statutes included tangible and intangible property and services, "including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, and transportation, except medicine or religious materials." *Id.* § 2339A(b)(1).

131. *See* Jennifer A. Beall, *Are We Only Burning Witches? The Antiterrorism and Effective Death Penalty Act of 1996's Answer to Terrorism*, 73 IND. L.J. 693, 694–95 (1998). The primary terror attack motivating the passage of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) was the 1995 bombing in Oklahoma City, Oklahoma. *Id.* The bombing of a federal building in the city killed 167 people. *Id.* at 693 n.1; *see also* Carlos F. Concepcion & Johanna Oliver Rousseaux, *Evolution of the ATA and Third-Party Liability for Terrorist Acts*, IN-HOUSE DEF. Q. 2–3 (Winter 2017), http://www.jonesday.com/files/Publication/96762fcf-3cb0-40ee-9ceb-d59e217ca9fb/Presentation/PublicationAttachment/5c394a82-eb45-4a0b-9e86-d9969ac8206d/IDQ-2017-01-Evolution%20of%20the%20ATA.pdf (tracing the continued evolution of the ATA in the face of additional terror attacks).

provisions that impose liability at an early stage."[132] In the years since their passage, these provisions have come to play a significant role in counterterror litigation.[133] Section 2339A provides a cause of action for providing material support to individual terrorists.[134] Section 2339B provides more broadly for action against individuals who provide any material support to a known foreign terrorist organization (FTO).[135] Under this provision, anyone who conspires to or knowingly provides material support or resources to a FTO, while either knowing it is a designated FTO or that it has or is engaging in terrorist activity or terrorism, faces fines and a substantial prison term.[136]

While originally intended to create criminal liability, this section, taken together with § 2333A's civil liability provision, as established in the original ATA, also exposes providers of material support to civil liability at the hands of the victims of those to whom they chose to provide material support.[137] In 2010, the Supreme Court substantially lowered the threshold for bringing such suits with its divisive 6–3 decision in *Holder v. Humanitarian Law Project*.[138] The case involved whether a nonprofit organization's provi-

132. Klein & Flinn, *supra* note 24, at 74.

133. Nicole Hong, *'Material Support' Statute is Front and Center in Antiterror Push*, WALL STREET J. (May 27, 2015, 7:25 PM), http://www.wsj.com/articles/material-support-statute-is-front-and-center-in-antiterror-push-1432719002.

134. 18 U.S.C. § 2339A.

135. *Id.* § 2339B.

136. *Id.* ("Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization[,] . . . that the organization has engaged or engages in terrorist activity[,] . . . or that the organization has engaged or engages in terrorism . . . ."). The U.S. Department of State maintains a list of designated foreign terror organizations, the support of which will lead to liability under this provision. *See Foreign Terrorist Organizations*, U.S. DEP'T ST., https://www.state.gov/j/ct/rls/other/des/123085.htm (last visited Oct. 3, 2018).

137. CHARLES DOYLE, CONG. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. § 2339A AND § 2339B 12 (Dec. 8, 2016).

> Nevertheless, 18 U.S.C. §2333 authorizes such suits for those injured in their person, property, or business by an act of international terrorism. The courts have concluded that the violations of . . . Section 2339B may constitute "acts of international terrorism" for purposes of Section 2333. They do so by construing violations of Section 2339A or Section 2339B as acts of "international terrorism" as defined in 18 U.S.C. §2331(1).

Id. (footnotes omitted).

138. 561 U.S. 1, 8, 21 (2010); *see also* Holder v. Humanitarian Law Project, GLOBAL FREEDOM EXPRESSION, https://globalfreedomofexpression.columbia.edu/cases/holder-v-humanitarian-law-project/ (providing an in-depth analysis of the *Holder* decision and its impact) (last visited Oct. 3, 2018).

sion requiring training in conflict resolution and various forms of political advocacy to a designated foreign terrorist organization violated the material support provision.[139] The central issue in the case turned on whether a nonprofit's general support to a terror organization, even if it would not further the organization's terrorist ends, qualified as material support under this provision.[140] In reaching a decision, the Court looked to the original congressional intent underlying § 2339B and, in light of this, subsequently interpreted the intent requirement of this provision as simply "knowledge about the organization's connection to terrorism, not specific intent to further the organization's terrorist activities."[141] This interpretation further broadened the provision's potential applications and the types of suits that could be brought under it, opening the door to potential liability for social media companies who provide support to known terrorist organizations, even when the company has no intent to further the organization's terrorist ends.[142]

In the years since the passage of § 2339, Congress has continued to hone and amend its anti-terror legislation, most recently and notably with the Justice Against Sponsors of Terrorism Act (JASTA) in 2015.[143] A bipartisan bill primarily focused on jurisdictional expansion of subject matter, JASTA's passage held particularly significant implications for the civil liability of terrorists and their supporters.[144] Congress intended it to "provide

139. *See Holder*, 561 U.S. at 10–11.

140. *Id.* at 1.

141. *Id.* at 16–17. "Congress plainly spoke to the necessary mental state for a violation of § 2339B, and it chose knowledge about the organization's connection to terrorism, not specific intent to further the organization's terrorist activities." *Id.*

142. *See* Emily Goldberg Knox, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295, 308 (2014) (discussing prosecution of social media companies under the material support provisions of the ATA). Although it has not yet been used with success against a social media company, the Department of Justice has utilized the material support provision of § 2339B to hold websites responsible for hosting terrorist material and to prosecute their leadership. *See id.* at 308–09.

143. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016) (codified at 18 U.S.C. § 2333, amending the Antiterrorism Act of 1990) [hereinafter JASTA]. JASTA was a uniquely bipartisan bill, which passed both the House and Senate without debate. Elura Nanos, *Bill Allowing Terror Victims to Sue Saudi Arabia Creates Serious Potential Problems*, LAW & CRIME (Sept. 28, 2016, 12:43 PM), https://lawandcrime.com/important/bill-allowing-terror-victims-to-sue-saudi-arabia-creates-serious-potential-problems-2/. President Obama attempted to veto it, but the Senate voted to override his veto. *Id.*

144. Nanos, *supra* note 143. The most controversial element of JASTA was that it withdrew sovereign immunity from nations facing charges for supporting terrorism, enabling victims to demand damages from a state sponsor of terror as well as the individual or organization responsible for their injuries. *See id.* It significantly expanded the federal subject matter jurisdiction in terror cases. *Id.*

civil litigants with the broadest possible basis" for seeking to recover damages against individuals, entities and even foreign countries, "wherever acting and wherever they may be found," that have provided direct or indirect material support to "foreign organizations or persons that engage in terrorist activities against the United States."[145]

The intentional breadth of this newly added provision encouraged courts and civil claimants to move more aggressively against actors of terror and their supporters.[146] In addition to more clearly establishing a general basis for civil suits for material support, JASTA opened the door to secondary liability claims in terrorism litigation, creating liability for aiding and abetting as well as civil conspiracy.[147] However, the creation of these secondary liability claims overlaps with prior and continued primary liability claims brought under the pre-existing material support provisions.[148] Accordingly, it remains to be seen exactly how these secondary liability claims will impact civil liability theories utilized against social media companies in cases going forward.[149]

To date, the approach most frequently taken by terror victims looking to recover for damages resulting from actors who aided in the execution of a terror attack in some secondary way remains the pursuit of a remedy under JASTA for reckless or knowing violations of one or more of the broad categories of material support activities prohibited under the material support statutes.[150] The civil cause of action for material support under JASTA

145. JASTA, 130 Stat. § 2(b).

146. *See JASTA: Expanded Liability Under US Anti-Terrorism Act*, CLIFFORD CHANCE 1 (Sept. 29, 2016), https://www.cliffordchance.com/briefings/2016/09/jasta_expanded_liabilityunder.html (follow "Download PDF" hyperlink) [hereinafter *Expanded Liability*]; *see also* JASTA, 130 Stat. § 2(a)(1), (7) ("The United States has a vital interest in providing persons and entities injured as a result of terrorist attacks committed within the United States with full access to the court system in order to pursue civil claims against [all who support terrorism].").

147. *Expanded Liability*, *supra* note 146, at 1. This became the first time that Congress explicitly clarified that theories of secondary liability could be used in civil actions against FTOs. *Id.*

148. *Id.*

149. *See id.* at 2 ("Whether JASTA's recognition of secondary liability will actually expand liability under the ATA is uncertain, since a number of courts have imposed primary liability on defendants for providing material support to terrorists, including providing financial or other services to terrorist organizations.").

150. *See supra* notes 127–42 and accompanying text; *see also* Brown, *supra* note 23, at 16–17 (discussing arguments for holding social media companies civilly liable for supporting ISIS). Material support liability theories have been pursued more often. Brown, *supra* note 23, at 16–17. Additionally, the material support provisions are specifically tailored to address issues relating to terrorists and their supporters, while more general secondary liability theories have yet to be frequently applied in this context. *Id.* As discussed previously, §§ 2339A–2339B detail examples of the types

serves as the foundation for the increasing number of suits being brought against social media companies for their provision of material support to terrorist organizations in recent years.[151] It has become increasingly apparent that social media sites today constitute one such major supporter, and where their actions lead to the loss of lives, they too bear responsibility.[152]

B. Establishing "Material Support" to Terrorists by Social Media Sites

The general civil cause of action for material support created under the ATA and JASTA does not establish specific elements that must be proven.[153] Accordingly, litigants and the courts turn to general principles of tort law to understand what must be proven to establish liability in such cases.[154] To bring a successful claim for material support, there must be (1) an unlawful action (in this case, the provision of material support); (2) the requisite mental state; and (3) causation.[155] As previously discussed, the nature of "material support" is incredibly—and intentionally—broad.[156] In general, the services provided by social media platforms easily satisfy this element.[157]

Establishing the element of *mens rea*, or state of mind, presents more of

---

of material support for which individuals may be held liable. *Expanded Liability*, *supra* note 146, at 2.

151. *See* JASTA, 130 Stat. § 2(b).

152. Nicholas Watt & Patrick Wintour, *Facebook and Twitter Have 'Social Responsibility' to Help Fight Terrorism, Says David Cameron*, GUARDIAN (Jan. 16, 2015, 9:00 AM), https://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat. Social media sites bear a social responsibility to ensure that they do not provide a safe space for terrorism to grow. *Id.*

153. Brown, *supra* note 23, at 17; *see also* Molzof v. United States, 502 U.S. 301, 305–07 (1992) (holding that the meaning of statutory language must be interpreted in light of the established common law principles against which Congress legislates).

154. *See* Wultz v. Islamic Republic of Iran, 755 F. Supp. 2d 1, 55 (D.D.C. 2010) (discussing how Congress did not expressly set out elements and, instead, intended to "incorporate general principles of tort law" into the ATA's civil cause of action).

155. Brown, *supra* note 23, at 17.

156. *See supra* note 145 and accompanying text; Brown, *supra* note 23, at 17–18 ("Establishing the provision of material support is the lowest hurdle when it comes to claims against social media . . . . A service that offers individuals and organizations the ability to network and communicate fits neatly into the . . . definition [of material support].").

157. See *infra* Section V.A for a discussion of particular theories for establishing material support to terrorism by social media platforms; *cf.* Knox, *supra* note 142, at 308 (discussing holding website administrators criminally liable for terrorist activities on their website). The "material support" of social media companies may be predicated on any number of the theories laid out in § 2339, including service, intangible property, and communications equipment. *See* 18 U.S.C. § 2339A(b)(1) (2012).

a challenge.[158] It also serves as the primary differentiator between meeting the requirements for material support in § 2339A and § 2339B.[159] Section 2339A requires either the defendant's actual knowledge that the material support in question would be used in preparing for or carrying out certain criminal violations or that the defendant intended for the support to be used for that purpose.[160] In other words, the material supporter needs to actually know that his actions will directly contribute to conducting an attack.[161] This actual knowledge requirement greatly limits the applicability of § 2339A's material support provision and, in the context of attempting to hold large social media companies liable, makes it untenable.[162] Attempting to show that a social media company specifically knew and intended to support a terrorist organization in their implementation of an attack is neither practical nor generally an accurate representation of the acts of those companies—or the reasoning behind holding them liable.[163]

However, the standard set by the material support provision under § 2339B is much broader.[164] Under this provision, the requisite *mens rea* is satisfied by establishing knowledge that material support or resources are being provided to terrorists or a FTO—not that they are actually being used to accomplish terrorist ends.[165] Accordingly, this element may be easily es-

158. *See* Brown, *supra* note 23, at 19–20. *Mens rea* is not explicitly included in the civil cause of action established by JASTA. *Id.* at 19. However, it is imposed based on the text of the two material support provisions and their subsequent interpretation and application. *Id*. In fact, "the critical question in any given case will be whether knowingly allowing terrorists to use the service can be viewed as material support." *Id.*

159. *See* 18 U.S.C. §§ 2339A–2339B.

160. *Id.* § 2339A.

161. *See id.*

162. Brown, *supra* note 23, at 19 ("This section presents an immediate—and likely insurmountable—hurdle for many plaintiffs . . . .").

163. Knox, *supra* note 142, at 308 ("Without direct evidence, it would be far-fetched to assert that legitimate businesses, such as social media companies, act intending to promote federal terrorism crimes."). Because of this high hurdle, § 2339A will be set aside for purposes of continuing discussion; however, much of the subsequent discussion regarding § 2339B and its application could be equally relevant to § 2339A. Many times claimants take the approach of "covering their bases," and choose to allege causes of action under both provisions. *See, e.g.*, Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150 (N.D. Cal. 2017) (alleging civil causes of action under both material support provisions). However, as of yet, no case has ever alleged that a mainstream social media site actively intended to contribute to a terror attack. *See generally* Knox, *supra* note 142, at 304–05 (discussing the potential difficulty for a plaintiff to satisfy the intent requirements of §§ 2339A and 2339B).

164. *See supra* notes 141–42 and accompanying text.

165. 18 U.S.C. § 2339B. Sections 2339A and 2339B provide two alternative means to the same end result of liability for material support. Norman Abrams, *The Material Support Terrorism Offenses: Perspectives Derived from the (Early) Model Penal Code*, 1 J. NAT'L SECURITY L. & POL'Y.

tablished.[166] In *Boim v. Holy Land Foundation for Relief and Development*, the court explained that even deliberate indifference as to whether an organization or individual engages in terrorism is sufficient to satisfy the state of mind requirement of § 2339B.[167] In *Boim*, the parents of an American citizen shot in Israel by alleged supporters of a terrorist organization filed claims against the organization and various other contributors to their son's murder.[168] The court in that case concluded that deliberate indifference generally requires only that an individual knows "there is a substantial probability that the organization engages in terrorism . . . [and] does not care."[169] If this is satisfied, then *mens rea* is easily met for purposes of material support liability.[170]

The standard required to demonstrate causation—the final element that must be satisfied—remains the center of substantial debate and is generally the most difficult to satisfy.[171] To date, the standard for what is reasonable in this context remains undetermined and has been interpreted in conflicting manners by the lower courts.[172] A standard of "but-for" causation is broadly viewed as being unreasonably high in this context; in other words, it is widely agreed that the material support need not have been so central that some attack or action would not have happened without it.[173] It is also broadly

5, 6 (2005) ("[Both] [t]hese provisions can be used to impose punishment for conduct remote from the commission of criminal harms, often conduct involving minimal and outwardly non-criminal acts.").

166. *See, e.g.*, Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 698 (7th Cir. 2008) ("[I]f you give money to an organization that you know to be engaged in terrorism, the fact that you earmark it for the organization's nonterrorist activities does not get you off the liability hook . . . .").

167. *Id.* at 693.

168. *Id.* at 688–89.

169. *Id.* at 693.

170. *Id.* at 721 ("State of mind requirement: the defendant must either know that the donee organization (or the ultimate recipient of the assistance) engages in such acts, or the defendant must be deliberately indifferent to whether or not it does so.").

171. Brown, *supra* note 23, at 26–27 (noting that there is a circuit split over the standard for proving causation).

172. Ronbert H. Schwartz, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*, 48 LOY. U. CHI. L.J. 1181, 1201 (discussing the varying opinions of the circuits regarding causation in material support cases). Each circuit court has its own interpretation of what "causation" means in the context of material support litigation. *Id.* The Seventh Circuit uses a more relaxed standard, looking at whether the party contributed to wrongdoing as a whole. *Id.* In contrast, the Second Circuit requires that the material support be a "substantial factor" in bringing about the resulting harm. *Id.* This appears to be the approach that more courts are tending to adopt. *See id.*

173. *See* Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 507 (E.D.N.Y. 2012) (recognizing that § 2333 does not require "but-for" causation). Proximate causation is all that is required under general tort law, and accordingly, the court found that it is all that is required in this context. *Id.* at 507–

agreed that *some* level of proximate cause is required; however, neither Congress nor case law has established a universal standard to apply.[174] This leaves the door open for terror victims to utilize this statute in seeking to hold social media companies liable; but it also leaves these potential plaintiffs with a great deal of uncertainty as to what they would need to allege to bring a successful claim.[175]

C. Establishing Secondary Liability of Social Media Sites for Terrorist Activity

The secondary liability for aiding and abetting and conspiracy, created under JASTA, provides a potential alternate route to a similar end.[176] In light of recent challenges in establishing material support as a cause of action for conduct on social media, it may well be that the plaintiffs should turn their attention toward alleging more cases under this theory.[177] Under § 2333(d)(2), civil suits may now be brought against any person who "aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."[178] Congress explicitly discussed the appropriate standard for imposing such liability, referring to the secondary liability standards set forth by the D.C. Circuit in *Halberstam v. Welch*.[179] *Halberstam* involved the criminal sec-

---

08.

174. *See* Schwartz, *supra* note 172, at 1200–02. Cases alleging social media companies to be material supporters of terrorism have taken a variety of approaches to this causation issue. *Id.* Based on decisions thus far, it appears that, in such instances, the courts are inclined to require a higher level of causation. *See id.*

175. *See generally* Fields v. Twitter, 881 F.3d 739 (9th Cir. 2018) (addressing proving causation in this context). In *Fields*, the Ninth Circuit held that proximate cause requires showing "some direct relationship" with the injury. *Id.* at 744. However, what must be shown to establish that "direct relationship" is not entirely clear. *See, e.g.*, Gonzalez v. Google, Inc., No. 16-cv-03282-DMR, 2018 WL 3872781, at *14 (N.D. Cal. Aug. 15, 2018) ("*Fields* did not address the standards applicable to claims brought pursuant to section 2333(d) . . . .").

176. See *supra* Section III.C for a discussion of the secondary liability created under JASTA; *see, e.g.*, *Fields*, 881 F.3d at 749–50 (holding that there is no liability because proximate cause did not exist); Force v. Facebook, Inc., 304 F. Supp. 3d 315, 332 (E.D.N.Y. 2018) (denying motion to amend complaint where parties did not cure defects in their arguments); Pennie v. Twitter, Inc., 281 F. Supp. 3d 874, 876 (N.D. Cal. 2017) (finding no liability where the plaintiffs failed to successfully allege causation).

177. *See Expanded Liability*, *supra* note 146, at 2 (explaining how social media companies "would be well-served to re-evaluate" due to JASTA's expansion of civil liability for terror attacks).

178. 18 U.S.C. § 2333(d)(2) (2012).

179. *See Expanded Liability*, *supra* note 146, at 2; Halberstam v. Welch, 705 F.2d 472, 486–88 (D.C. Cir. 1983). *Halberstam* laid out a framework for understanding general secondary liability,

ondary liability of a burglar's accomplice.[180] The case laid out in detail the requirements to establish liability as both an aider and abettor and member of a conspiracy—requirements Congress now specifically recognizes as applicable in a material support context.[181] Civil conspiracy can be established where (1) an agreement exists between two or more individuals to participate in either (a) an unlawful act or (b) a lawful act in an unlawful manner; (2) the actions of one of the co-conspirators caused an injury to another; and (3) that action occurred pursuant to accomplishing the "common scheme" of the conspiracy.[182] Liability for aiding and abetting, meanwhile, comes into play any time (1) the party whom the defendant aids performs a wrongful act that causes an injury; (2) that defendant is generally aware of his role as part of an overall illegal or tortious activity when he provides the assistance; and (3) his actions knowingly and substantially supports the principal violation.[183] In theory, the imposition of secondary liability claims means victims can now bring additional suits against material supporters of FTOs, including social media companies.[184] The creation of these secondary liability claims overlaps with prior and continued primary liability claims brought under the already-existing material support provisions.[185] Accordingly, how they will, in practice, expand the scope of suits to be brought remains to be seen. However, regardless of whether plaintiffs attempt to hold a social media company accountable under a primary or secondary liability theory, they will encounter the same ultimate road block: § 230 of the Communications Decency Act.[186]

IV. CHALLENGES PROHIBITING VICTIMS FROM IMPOSING CIVIL LIABILITY ON SOCIAL MEDIA COMPANIES

Regardless of the theories of liabilities used, any attempt by victims of terror to hold social media companies liable as material supporters faces a

explaining both aiding and abetting and civil conspiracy. *Id.*

180. *Halberstam*, 705 F.2d at 474–75. The case involved the appeal of the conviction by one of two individuals involved in a joint burglary and murder. *Id.* The circuit court sought to "determine the civil liability of the passive but compliant partner" of the primary criminal actor and ultimately found her liable under both a criminal conspiracy or aider-and-abettor theory. *Id.* at 474, 489.

181. *Expanded Liability*, *supra* note 146, at 1–2.

182. *Halberstam*, 705 F.2d at 477.

183. *Id.*

184. *Expanded Liability*, *supra* note 146, at 2.

185. *Id.*

186. *See infra* Part IV.

major challenge in the form of § 230 of the Communications Decency Act (CDA).[187] The CDA, even more definitively than the ambiguous causation requirements currently imposed, is the biggest barrier to allowing victims to recover from these companies.[188]

A. The Communications Decency Act

When Congress passed the Telecommunications Act of 1996, it included what would become known as § 230 of the CDA in order to address new issues of third-party liability raised by the internet's advent and the plethora of new legislation being developed to understand and regulate it.[189]

1. History and Congressional Intent Behind the CDA

Senator James Exon first introduced a draft of what would eventually become the CDA as one piece of the Telecommunications Act of 1996.[190] Exon brought the act before Congress with a very specific issue and agenda in mind; namely, he wanted to address the public policy concerns associated with the easy availability of internet pornography and, in particular, its accessibility to—and impact on—minors.[191] From Exon's perspective, "[t]he fundamental purpose of the [CDA was] to provide much needed protection for children."[192] However, the CDA, as Exon originally proposed it—while supported almost unanimously in theory—raised serious concerns, in practice, that its breadth would significantly infringe on the First Amendment

187. *See* 47 U.S.C. § 230 (2012).

188. *See* Schwartz, *supra* note 172, at 1203 ("[E]ven if a plaintiff satisfies the proximate cause element, the plaintiff must still hurdle the CDA immunity defense."). Senator James Exon introduced the overall provision as a revision to 47 U.S.C. § 223. Patricia Spiccia, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 VAL. U. L. REV. 369, 380–81 (2013); *see also* Claudia G. Catalano, Annotation, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C.A. § 230*, 52 A.L.R. Fed. 2d 37 (2011) ("Congress enacted the Communications Decency Act (CDA) in part to carve out a sphere of immunity from liability for providers of interactive computer services to preserve that 'vibrant and competitive free market' of ideas on the Internet.").

189. Christopher Zara, *The Most Important Law in Tech Has a Problem*, WIRED (Jan. 3, 2017, 12:00 AM), https://www.wired.com/2017/01/the-most-important-law-in-tech-has-a-problem/.

190. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 52–53 (1996).

191. *Id.* at 53 ("Senator Exon was motivated out of a concern for the proliferation of pornography and indecency on the Internet and the easy access to that material by the youth of America.").

192. 141 CONG. REC. S8088 (daily ed. June 9, 1995) (statement of Sen. Exon).

rights of internet platforms and providers if passed.[193]

In order to address these concerns, the House presented an amendment to § 223 of the CDA that eventually became codified as § 230.[194] Section 230 was intended to shield internet providers from taking on liability when they choose to filter indecent content and to establish that, as a matter of public policy, the federal government is not in the business of affirmatively regulating internet content.[195] Section 230(c)(2) addressed avoiding affirmative liability for censoring inappropriate content.[196] The provision "removes all disincentives for using filtering software, directly immunizing interactive computer services for voluntary acts of filtering or making such technology available."[197] However, it is § 230(c)(1) that has caused the most significant debate and conflict in the years since its passage.[198] Section 230(c)(1) states that, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[199]

The very day §§ 223 and 230 passed, § 223 became the subject of a lawsuit.[200] Subsequently, significant portions of that provision—the very one which § 230 was created to supplement—were discarded as unconstitutionally overbroad.[201] The Court found that § 223 reached protected materials and threatened to destroy the unique and participatory nature of the internet.[202] Thus, § 223 was repealed, but § 230 remained an active part of the

193. Cannon, *supra* note 190, at 67, 75–88; *see* Ryan French, *Picking Up the Pieces: Finding Unity After the Communications Decency Act Section 230 Jurisprudential Clash*, 72 LA. L. REV. 443, 446 (2012).

194. French, *supra* note 193, at 446–52 (discussing the purpose and development of § 230).

195. *Id.* at 448; *see also* 141 CONG. REC. 22,045 (1995) (remarks of Rep. Cox).

196. *See* 47 U.S.C. § 230(c)(2) (2012) ("No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].").

197. Paul Ehrlich, *Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401, 410 (2002).

198. *See* 47 U.S.C. § 230(c)(1); *see also* French, *supra* note 193, at 449–50 (discussing the purpose of this provision); Zara, *supra* note 189 ("[T]his landmark piece of legislation is often cited as the most important tool ever created for free speech on the internet.").

199. 47 U.S.C. § 230(c)(1).

200. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 861 (1997).

201. *Id.* at 882–85; *Court Rules CDA Unconstitutional*, FINDLAW, http://technology.findlaw.com/networking-and-storage/court-rules-cda-unconstitutional.html (last visited Oct. 6, 2018).

202. *Reno*, 521 U.S. at 849–53.

implemented Telecommunications Act, now subject to an interpretation devoid of its original purpose or context.[203] Subsequently—and likely because of that lack of context—this provision and its proper application became a significant topic of debate amongst the circuits.[204] The Fourth Circuit became the first to provide a significant analysis of the proper application of the statute, holding that, in order to respect the importance of free speech, § 230's interpretation should be extremely "broad," thereby providing extensive grounds for immunity.[205] However, soon after that opinion, the Seventh Circuit took a very different stance, questioning whether § 230 actually provides any immunity whatsoever to computer providers.[206] The Ninth Circuit appeared to fall somewhere in between the polarizing views of the other circuits when it weighed in, finding that—while § 230 may indeed create some immunity—that immunity is abrogated as soon as the service provider becomes a contributor to the third-party's content.[207]

That said, while conflict remains, construction of § 230 immunity has historically been very broad—and arguably far too broad.[208] Section 230 currently serves as the best source of protection for internet service providers (ISPs).[209] There is growing concern among scholars and dissenting courts that this sweeping protection actually defeats the policy purposes § 230 intended to further and needs to be either updated or done away with altogether.[210] These skeptics focus on the point that § 230 intended to eliminate disincentives to self-regulation that had been previously created by case law and, subsequently, to actually *incentivize* self-regulation measures.[211] How-

203. *See generally id.* at 864, 887 (finding that § 223 was unconstitutionally overbroad and infringed upon free speech).

204. French, *supra* note 193, at 451–56.

205. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

206. *See* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003).

207. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168–69 (9th Cir. 2008) (recognizing loss of immunity "if [a website] contributes materially to the alleged illegality of the conduct").

208. *See generally* Spiccia, *supra* note 188, at 392–95.

209. *Id.* at 399 ("Although section 230 has garnered a great deal of criticism since it was passed, it remains the primary source of protection for ISPs today.").

210. *Id.* at 395–96. These concerns are not limited to the context of material support litigation. *See* Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505, 1505–06 (2015). Section 230's broad interpretation today threatens to offer too much protection, even protecting social media sites that are permitting defamation. *Id.* at 1505. An increasing number of individuals are advocating for either an alteration in interpretation—or revisions to the statutory provision itself. *Id.*

211. *See* H.R. REP. NO. 104–458, at 194 (1996) ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such pro-

ever, this protection has failed to effectively motivate consistent self-regulation by ISPs.[212] Thus, while Congress intended § 230 to provide protection for "Good Samaritan" self-regulation, the unintended side effect has been to inspire passivity and protect belligerence.[213]

The result of this is that § 230 both directly thwarts its own intended purpose to encourage a system of self-regulation and positive incentivization, and simultaneously fails to adequately protect victims of internet crimes.[214] Frustration over the current application of § 230's immunity provision has grown as the immunity becomes an impediment in suits involving circumstances that were unconsidered and unforeseeable by Congress at the time of its creation.[215] In particular, it has served as the repeated and determinative roadblock to holding social media platforms liable for their actions

viders and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

212. Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 U. PITT. J. TECH. L. & POL'Y 3, 26 (2007) ("It is counterproductive to attempt to encourage these entities to self-regulate their content for defamatory speech by immunizing them for that defamatory speech *regardless of whether the ISP attempts whatsoever to be responsible and screen its content*. While we would like to think that ISPs will screen their own content out of the goodness of their corporate hearts, it is a risk that Congress has chosen to take without any evidence. With this choice, Congress has put its faith in ISPs to self-regulate and has cut off individuals' ability to seek redress, regardless of whether those ISPs regulate their content.").

213. Spiccia, *supra* note 188, at 405 ("[T]he law as it stands today protects not only self-regulating Good Samaritans, but also those ISPs that refuse to self-regulate; therefore, no incentive exists for ISPs to behave like the Good Samaritans Congress sought to protect when it passed the statute."); *see also* Sewali K. Patel, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 684 (2002) ("Common sense dictates that an ISP will not waste its time and money monitoring content over the Internet when it will suffer no repercussions from failing to do so.").

214. *See* Spiccia, *supra* note 188, at 409–10. The types of internet crimes with which critics of this provision were traditionally concerned included more traditional torts, including issues related to defamation and publication of lewd content. *Id.*

215. *Id.* at 396 ("[N]umerous critics have also voiced concerns regarding the broad protection section 230 provides, arguing that the statute has failed to achieve its main objective because ISPs receive immunity regardless of whether they regulate, so they have no incentive to do so."). Social media and its use by terrorists were not issues of concern at the time of § 230's passage. *See generally* Cannon, *supra* note 190 (outlining the legislative history of the CDA and Senator Exon's motivations for proposing it). However, its language serves as a central issue in modern suits against social media companies in this context. *See* Andrew O'Reilly, *Exclusive: Families of Orlando Nightclub Shooting Victims Sue Facebook, Twitter, and Google*, FOX NEWS (Dec. 19, 2016), http://www.foxnews.com/us/2016/12/19/exclusive-families-orlando-nightclub-shooting-victims-sue-facebook-twitter-and-google.html ("At the heart of the lawsuit is the interpretation of a provision tucked deep inside the Communications Decency Act (CDA) of 1996 called section 230.").

in a variety of contexts.[216] This issue has arisen in the context of cyberbullying, gang recruitment, human trafficking recruitment and marketing, as well as now in the context of terrorist recruitment and coordination.[217] In some contexts, despite pressure from the tech industry to maintain the breadth of § 230 immunity, Congress has already begun to narrow the scope of this immunity.[218] Most recently, in March 2018, Congress passed a bill that explicitly exposes internet providers to expanded liability in the human trafficking context by providing that "[it is] a crime to knowingly benefit from knowing conduct that by any means assists, supports or facilitates an action" that supports human trafficking.[219] The bill, specifically aimed at removing CDA protection from ISPs, entirely and explicitly abrogates the immunity clause in the human trafficking context.[220] Its impact has been immediate.[221] However, in other contexts—and particularly in terms of the liability of social media companies for their contributions to terrorism—Congress has re-

216. *See* O'Reilly, *supra* note 21; *see also* cases cited *supra* note 176 (noting courts' difficulty in holding social media platforms liable for harms from terror organizations).

217. *See* Michael S. Isselin, *#StopImmunizing: Why Social Networking Platform Liability Is Necessary to Provide Adequate Redress for Victims of Cyberbullying*, 61 N.Y. L. SCH. L. REV. 369, 389 (2017) (finding that "[t]he benefits of this [liability creating] process far outweigh any drawbacks" in the context of fighting cyberbullying); Shannon Dolan, *Combating a Never Ending Battle: Online Human Trafficking and the Communications Decency Act*, SETON HALL L. SCH. STUDENT SCHOLARSHIP (2017) (discussing generally the impact of CDA immunity on online human trafficking); Joseph Monaghan, *Social Networking Website Liability for the Illegal Actions of Its Users*, SETON HALL L. SCH. STUDENT SCHOLARSHIP (2011) (discussing social media liability under the CDA for sexual abuse, cyberbullying, and gang activity).

218. *See, e.g.*, Reuters, *House Passes Sex-Trafficking Bill Despite Tech Opposition*, N.Y. POST (Feb. 28, 2018, 9:35 AM), https://nypost.com/2018/02/28/house-passes-sex-trafficking-bill-despite-tech-opposition/ ("The US House of Representatives . . . overwhelmingly passed legislation [in February 2018] to make it easier to penalize operators of websites that facilitate online sex trafficking, chipping away at a bedrock legal shield for the technology industry.").

219. Daphne Keller, *What Does the New CDA-Buster Legislation Actually Say?*, CTR. INTERNET & SOC'Y (Aug. 11, 2017, 11:32 AM) (emphasis omitted), http://cyberlaw.stanford.edu/blog/2017/08/what-does-new-cda-buster-legislation-actually-say. The Stop Enabling Sex Traffickers Act (SESTA), packaged with Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), targeted internet sites that were enabling the continuation of sex trafficking and specifically focused on the irreputable site Backpage.com. Haley Halverson, *Ending Immunity of Internet-Facilitated Commercial Sexual Exploitation Through Amending the Communications Decency Act*, 21 J. INTERNET L. 3, 8–9, 12 (2018); *see* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L No. 115-164, 132 Stat. 1253 (2018).

220. *See* Keller, *supra* note 21. Opponents of the bill expressed concern that "SESTA opens doors to an unforeseeable array of claims, against an unforeseeable array of defendants." *Id.*

221. *See, e.g.*, Niraj Chokshi, *Missed Connections: Craigslist Drops Personal Ads Because of Sex Trafficking Bill*, N.Y. TIMES (Mar. 23, 2018), https://www.nytimes.com/2018/03/23/business/craigslist-personals-trafficking-bill.html (reporting that Craigslist shut down its personal ads the very week SESTA passed).

mained silent, leaving the proper scope of the immunity clause an issue of significant debate in the courts.[222]

2. Analysis of Competing Views of the CDA's Proper Role

Understanding how the CDA does and should come into play in social media suits brought under §§ 2333 and 2339B is central to understanding the current state of the courts and case law today—and why a different direction needs to be taken in the future.[223] Currently, social media sites use § 230 as a hiding place; it is seen as the fail-safe "fallback" argument that cannot be lost.[224] However, this view is not based in a proper interpretation of the congressional intent of this section, nor as a matter of policy, is it a view that should be perpetuated.[225] Social media companies assert that they are simply third-party content providers that cannot possibly be held liable because they are fully protected by § 230.[226] Accordingly, they argue, any assertion of liability arising under §§ 2333 and 2339B is moot.[227] Under recent judi-

222. *See* discussion *infra* Section IV.A.2.

223. See discussion *infra* Part V for explanation of suggested alterations to the text of the CDA and alternate methods of imposing liability by circumventing the CDA.

224. Lisa Matsue, *The Twentieth Anniversary of the CDA & the Changing Role of Social Media Companies*, FORDHAM INTELL. PROP., MEDIA & ENT. L.J. (Oct. 13, 2016), http://www.fordhamiplj.org/2016/10/13/the-twentieth-anniversary-of-the-cda-the-changing-role-of-social-media-companies/ ("Social networking platforms in particular have been heavily protected by the CDA.").

225. Jemima Kiss & Charles Arthur, *Publishers or Platforms? Media Giants May Be Forced to Choose*, GUARDIAN (July 29, 2013, 4:08 PM), https://www.theguardian.com/technology/2013/jul/29/twitter-urged-responsible-online-abuse ("Hiding behind a veil of free speech is not teaching users what freedom of speech is really about. There's an eerie newness to these type [sic] of very public, very humiliating and very confident attacks."). The subsequent discussion is predicated on the assumption that plaintiffs are attempting to bring suit while § 230 remains in its current form. See discussion *infra* Part VI for an analysis of whether § 230 should be kept or whether its modification or dissolution could potentially provide a better alternative.

226. *See* Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018, 5:11 AM), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change. Experts assert that "Section 230 has turned into a Teflon shield, not to protect free speech but to protect business revenue." *Id.*

227. *See* Christian P. Foote, *Web Publishers Must Exercise Caution to Protect Their Immunity Under the Communications Decency Act*, CARR MCLELLAN (May 11, 2017) (discussing "three situations where courts have held Section 230 moot because of the web publisher's own responsibility for developing the offending content"); *see, e.g.*, Russell Spivak, *Facebook Immune from Liability Based on Third-Party Content*, LAWFARE (May 23, 2017, 1:45 PM), https://www.lawfareblog.com/facebook-immune-liability-based-third-party-content (discussing how courts have found § 230 protects social media sites in the anti-terror context).

cial interpretation in the lower courts, this does seem to be a significant concern.[228]

However, CDA immunity for social media companies providing a service to terrorists is neither as impregnable nor as controlling as it originally seems.[229] The primary issue that arises in seeking to hold social media companies liable for material support comes in the apparent conflict between § 230 and § 2339B.[230] There are two means by which this conflict may be resolved: either one provision is preeminent over the other, or there is some reading that allows for their coexistence.[231]

The preferred method of resolving statutory conflict is generally to seek to reconcile the statutes by reading one or both as narrowly as possible, so as to give effect to both provisions without creating a conflict between them.[232] However, on a practical level, the most common interpretation of CDA does not leave room for these statutes to coexist.[233] Section 2339B says anyone who provides material support to FTOs is liable for civil suit.[234] Social media sites provide clear material support in the form of digital communication equipment and invaluable services to FTO affiliates.[235] However, under § 230, courts have interpreted social media's platform provision as not providing any third-party content, finding that, as a result of this, social media sites cannot be subjected to liability.[236] When two statutes irreconcilably conflict, courts traditionally look to the statutes' order of enactment, together

228. *See, e.g.*, Pennie v. Twitter, Inc., 281 F. Supp. 3d 874, 888 (N.D. Cal 2017) (finding CDA barred claims where the theory of liability "rests largely on the premise that Defendants should be held responsible for content created and posted by users"); Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150, 1170–71 (N.D. Cal. 2017) (finding CDA provided immunity where Plaintiffs failed to allege the social media company was an "information content provider").

229. Joshua R. Stein & John Delaney, *Controversial California Court Decision Significantly Narrows a Crucial Liability Safe Harbor for Website Operators*, SOCIALLY AWARE (Aug. 24, 2016), https://www.sociallyawareblog.com/2016/08/24/hassell/. In other areas of the law, courts have begun carving out exceptions to section § 230 immunity. *Id.* For instance, a recent California court decision held that § 230 did not preclude Yelp from being held liable for failing to remove defamatory posts. *Id.*

230. *See generally* Spivak, *supra* note 227.

231. *See* discussion *infra* notes 232–41 and accompanying text.

232. *See* Ricci v. DeStefano, 557 U.S. 557, 580 (2009) (interpreting conflicting provisions of Title VII of the Civil Rights Act of 1964 so as "to give effect to both provisions where possible").

233. Spivak, *supra* note 227. Under the current judicial trend, it appears increasingly unlikely that a civil claim under § 2333 which relies upon the content posted by a terrorist to find liability, will be able to withstand § 230's immunity scrutiny. *Id.*

234. 18 U.S.C. § 2339B (2012).

235. *See* discussion *supra* Section II.A.

236. *See* 47 U.S.C. § 230 (2012).

with any specific instructions about how to resolve conflicts between a given statute and other laws previously existing or later enacted.[237] The prioritization of the more recent statute is based on the well-established principle of the Last-in-Time Rule.[238] That is, the more recently legislated statute or case law most likely provides the best indicator of the current intent of Congress.[239] In this instance, both the most recent update to the material support statute in § 2339B, as well as the secondary liability provisions enacted under JASTA, passed years after the CDA.[240] Accordingly, where the CDA conflicts with liability imposed under the civil material support liability created under JASTA and the ATA, the anti-terror provision should prevail.[241]

Consideration of the purpose and content of the statutes at issue provides further support for this.[242] When a new policy is created by a subsequent federal statute, it should control construction and interpretation of earlier statutes.[243] Section 2333 is not only a subsequently embodied statute; it is a statute furthering a very specific—and significant—public policy concern.[244] Namely, it is a vital tool in the fight against terrorism and the pro-

237. *See* SmithKline Beecham Consumer Healthcare, L.P., v. Watson Pharm., Inc., 211 F.3d 21, 27–28, 28 n.3 (2d Cir. 2000).

238. *See* In re Ionosphere Clubs, Inc., 922 F.2d 984, 991 (2d Cir. 1990) ("[W]hen two statutes are in irreconcilable conflict, we must give effect to the most recently enacted statute since it is the most recent indication of congressional intent."); Kevin M. Clermont, *Limiting the Last-in-Time Rule for Judgments*, 36 REV. LITIG. 1, 16–21 (2017) (outlining the emergence and development of the last-in-time rule among U.S. courts).

239. *See Ionosphere Clubs*, 922 F.2d at 991.

240. *See CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history (last visited Oct. 7, 2018). Section 230 came into effect in 1996. *Id.* Section 2339B was most recently amended in 2015. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub L. No 114–23, 129 Stat. 268 (2015). JASTA entered into effect on September 28, 2016. JASTA, Pub L. No.114–222, 130 Stat. 852 (2016) (codified at 18 U.S.C. § 2333, amending the Anti-terrorism Act of 1990).

241. *See* JASTA, 130 Stat. § 2(b). This is particularly true in light of JASTA's language providing for the "broadest possible basis" for liability. *Id.*

242. *See generally* Abrams, *supra* note 165 (outlining the background of the material support statutes).

243. *See* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 143 (2000) ("[A] specific policy embodied in a later federal statute should control . . . construction of the [earlier] statute, even though it ha[s] not been expressly amended." (quoting United States v. Estate of Romani, 523 U.S. 517, 530–31 (1998))).

244. *See* Laura B. Rowe, *Ending Terrorism with Civil Remedies: Boim v. Holy Land Foundation and the Proper Framework of Liability*, 4 SEVENTH CIR. REV. 372, 373 (2009), https://www.kentlaw.iit.edu/sites/ck/files/public/academics/jd/7cr/v4-2/rowe.pdf ("[T]he [ATA's] legislative history also indicates quite clearly that the purpose of § 2333 was to cut off, or significantly impair, vital sources of terrorist funding . . . ."). Imposition of civil liability against agents of

tection of national interests.[245] Social media companies are providing material support, and terror victims are attempting to hold them liable.[246] While future developments in social media could not be understood or anticipated at the time these provisions were created, their behavior today places them directly within the purview of the types of behavior that Congress intended the statute to preclude at the time of its creation.[247] In contrast, § 230 is a non-specific and overbroad provision that Congress created without any possible consideration of its potential ramifications on liability for supporting terror organizations twenty years later.[248] Accordingly, the reasonable means of reconciliation of these laws would appear to be straightforward, with § 230 treated as subordinate to the statutes creating material support liability.[249] However, while adopting such an approach appears both logical and effective from a policy perspective, courts to date have not recognized it as a viable option to circumvent the problem of § 230.[250]

This leaves plaintiffs to grapple with the attempted co-existence of the material support civil liability provisions and § 230.[251] In order for social media companies to be found liable for material support, then, they must be

terror is important, not only from the perspective of the victims who deserve to properly recover for their injuries, but also as a tool to fight terrorism. *Id.* ("[P]erhaps one of the most important and effective means of stopping terrorism is to cut off or significantly impair vital sources of funding . . . . Because Congress intended to enable private parties to attack terrorist funding through these civil suits, Congress created yet another tool for eliminating terrorism in general.").

245. *Id.* The material support provided by third-parties becomes, directly or indirectly, the basis of the FTO's ability to carry out attacks. *Id.* at 425. Specifically, the material support provided by social media companies to terrorists globally enables terrorist attacks through multiple means. *See supra* Part II for a discussion of how social media furthers terrorism. Such action is specifically what section 2333 seeks to punish. *See* Rowe, *supra* note 24, at 425.

246. *See, e.g.*, Force v. Facebook, Inc., 304 F. Supp. 3d 315, 323 (E.D.N.Y. 2018) ("The court sees no reason to conclude that the ATA impliedly abrogated Section 230.").

247. *See* JASTA, Pub. L. No. 114-222, § 2(b), 130 Stat. 852 (2016) (codified at 18 U.S.C. § 2333, amending the Antiterrorism Act of 1990) (seeking to provide terror victims as civil litigants "the broadest possible basis" for recovery).

248. *See id.*; 47 U.S.C. § 230 (2012).

249. *See supra* notes 232–50 and accompanying text.

250. *See Section 230 of the Communications Decency Act*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 (last visited Oct. 7, 2018) ("CDA 230 makes the U.S. a safe haven for websites that want to provide a platform for controversial or political speech and a legal environment favorable to free expression.").

251. *See Force*, 304 F. Supp. 3d at 323 (finding that "the two acts can be read without any conflict: Section 230 provides a limited defense to a specific subset of defendants against the liability imposed by the ATA"); Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150, 1168–71 (N.D. Cal. 2017) (noting that plaintiffs asserted Google constituted an "information content provider" based on its advertisements but failed to properly allege so "with respect to the information at issue, i.e., the offending ISIS videos," in the second amended complaint).

held liable for something other than their "publisher" function.[252] Plaintiffs have attempted several different means of establishing that social media defendants provided material support by means outside of their function as publishers.[253] These include resting liability on provision of accounts to FTOs and their followers and the addition of third-party content in the form of advertisements accompanying FTO members' posts or editing of the content posted by them.[254] Ultimately, however, whether any of these theories of liability will find success remains an open question that will necessarily be addressed in litigation, legislation, or both, in the coming months and years.[255]

B. Causation

Even if a plaintiff manages to overcome the daunting obstacle imposed by § 230's publisher immunity clause, satisfying the causation element of the material support claim remains a major challenge in its own right.[256] As discussed above, the standard of causation required to successfully bring allegations against a social media company for material support remains an ambiguous topic of dispute among the circuits.[257] Recently, in *Fields v. Twitter, Inc.*, the Ninth Circuit held that the proximate causation required by the "by reason of" language in JASTA's civil material support cause of action requires a plaintiff to establish "at least some direct relationship between the injuries . . . suffered and the defendant's acts."[258] This is a deviation from the standards applied by other courts that have found proximate cause in the material support context is satisfied wherever the resulting harm

252. *See* Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017). Courts have found that liability may be imposed in situations not "requir[ing] that the defendant be treated as the publisher or speaker of content provided by another." *Id.*

253. See *infra* Section VI.A for a discussion of potential theories of liability that circumvent the CDA challenges.

254. *See, e.g.*, Fields v. Twitter, Inc., 881 F.3d 739, 750 (9th Cir. 2018) (finding that the account provision theory failed, not because it was implausible, but because plaintiffs failed to allege facts sufficient to support it).

255. *See id.* In its recent *Fields* decision, the Ninth Circuit intentionally declined to hold on the CDA immunity issue with relation to liability for material support to terrorists, leaving the door open for further consideration and debate. *Id*.

256. *See, e.g.*, *id.* at 749–50 (holding plaintiffs failed to demonstrate proximate cause between Twitter and the attack that killed the decedent).

257. *See* discussion *supra* notes 171–75 and accompanying text; *see also Fields*, 881 F.3d at 744–48 (discussing different standards of proximate cause applied by the circuits in proximate causation).

258. *Fields*, 881 F.3d at 744.

is foreseeable.[259] The Seventh Circuit noted that "the *fact* of contributing to a terrorist organization rather than the *amount* of the contribution is the keystone of liability."[260] However, the plaintiffs in *Fields* alleged only the most general of relationships between Twitter's material support of terror and the specific incident resulting in the death of one of the plaintiff's spouse.[261] While the lack of clarity and specific facts of several of the cases brought thus far have not supported proximate cause under either standard, this is far more indicative of the weakness of those individual cases than evidence that proximate cause can never be satisfied in a social media material support case.[262]

What is needed are more cases alleging at least moderately specific facts that demonstrate direct connections between social media usage and subsequent injury.[263] For instance, in the *Force v. Facebook*[264] decision recently issued by a New York district court, the plaintiffs provided specific and detailed allegations against Facebook for acts that occurred during what is commonly referred to as the "Facebook Intifada" in Israel.[265] That case, brought by victims and families of victims killed in knife attacks inspired by

259. Benjamin Wittes, *Another Day, Another Material Support Suit Against a Social Media Company*, LAWFARE (Jan. 10, 2017, 4:55 PM), https://www.lawfareblog.com/another-day-another-material-support-suit-against-social-media-company. The Seventh Circuit standard of causation "seems more forgiving." *Id.* The Seventh Circuit also provides the best summary of the lower standard approach. *Id.*

260. Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 691 (7th Cir. 2008) (emphasis added).

261. *See Fields*, 881 F.3d at 750 ("The SAC does not articulate any connection between Twitter's provision of this aid and Plaintiffs–Appellants' injuries.").

262. *See, e.g.*, *id.* at 749. In *Fields*, the causal links alleged were admittedly weak. *See id.* "Plaintiffs allege no connection between the shooter, Abu Zaid, and Twitter. There are no facts indicating that [the terrorist]'s attack was in any way impacted, helped by, or the result of ISIS's presence on the social network." *Id.* at 750 (quoting Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1127 (N.D. Cal. 2016)).

263. *See* Benjamin Wittes & Zoe Beddell, *Facebook, Hamas, and Why a New Material Support Suit May Have Legs*, LAWFARE (July 12, 2016, 1:23 PM), https://www.lawfareblog.com/facebook-hamas-and-why-new-material-support-suit-may-have-legs. In the alternative, plaintiffs would need to show that the social media companies had actual knowledge of and resulting harm that occurred to the plaintiffs. *Id.*

264. *See generally* Force v. Facebook, Inc., 304 F. Supp. 3d 315 (E.D.N.Y. 2018) (dismissing for failure to show causation by acts not covered under the CDA immunity clause).

265. Wittes & Bedell, *supra* note 263. The "Facebook Intifada" is a period of time in Israel in the mid-2000s that involved a widespread outbreak of violence in Israel by lone-wolf attackers in conjunction with a significant social media press to publish videos glorifying bombings and knife attacks. *See* Shira Rubin, *This Latest Palestinian Uprising Is a Facebook Intifada*, USA TODAY (Oct. 15, 2015, 7:12 AM), https://www.usatoday.com/story/news/world/2015/10/14/latest-palestinian-uprising-facebook-intifada/73936190/.

social media postings made by the PLO during that period, was dismissed; however, the dismissal was not based on a failure to allege causation—but a failure to show causation by acts not covered under the CDA immunity clause.[266] The court held that, because the provision of support provided by social media sites was inherently "[b]ound up . . . in the content that [FTO]-affiliated users provide," the defendant's social media sites were protected by § 230 immunity.[267] The *Force* decision illustrates what may be the biggest challenge facing plaintiffs seeking to bring social media material support liability suits: courts have turned these cases into a vicious cycle.[268] When the courts do not want to address proximate cause, they rest their denials on the CDA, but when they do not wish to address the CDA, they credit their dismissals to a lack of causation.[269] The result is a growing body of ambiguous and circular case law which does nothing to clarify the circumstances in which a material support suit for social media sites could be brought or to establish a more determinative framework for the liability of such entities.[270]

V. PUBLIC POLICY IMPLICATIONS OF MATERIAL SUPPORT LIABILITY FOR SOCIAL MEDIA COMPANIES

The confusing body of case law and the consistent obstacles facing plaintiffs in these cases are particularly concerning in light of the public policy concerns raised by considering the liability of social media companies as facilitators of international terrorism.[271] Protecting the safety of American citizens and defending the national security are policy matters of the highest order.[272] At the same time, safety and security cannot come at the expense

266. *Force*, 304 F. Supp. 3d at 329–30; *see also* Benjamin Wittes & Zoe Bedell, *Did Congress Immunize Twitter Against Lawsuits for Supporting ISIS?*, LAWFARE (Jan. 22, 2016, 9:14 AM), https://www.lawfareblog.com/did-congress-immunize-twitter-against-lawsuits-supporting-isis ("The trouble, of course, is that it's pretty hard to imagine a plaintiff who could establish all of the elements required under § 2333 (particularly the causal relationship between the material support and the injury) without ever relying on the substance of third-party content.").

267. *Force*, 304 F. Supp. 3d at 329–30.

268. *See infra* text accompanying notes 269–70.

269. *See, e.g.*, Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150, 1170–71 (N.D. Cal. 2017) (declining a substantive ruling on causation where the court found CDA immunity).

270. *See, e.g.*, Fields v. Twitter, Inc., 881 F.3d 739, 750 (9th Cir. 2018) (refusing to hold on CDA immunity where there was no causation).

271. See *infra* Sections V.A–B for a discussion of the public policy concerns.

272. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 29–30 (2010) (noting Congress' specific findings regarding global terrorism and its status as a critical threat).

of free speech, which has been long established as a fundamental and compelling American value.[273] Thus, any solution to this issue requires a balancing act, finding a way to navigate these competing policy matters.[274]

A. National Security & Counter-Terrorism

After the increase in lone-wolf attacks over the past few years, the families of victims began to recognize the role that social media played in the loss of their loved ones.[275] John Carlin, the former Assistant Attorney General for National Security, noted that social media has created a new threat from terrorists.[276] "Here in America," he explained in an interview with the Public Broadcasting Service, "we're not seeing any particular ethnic group or geographic group answer the call [to terror]. Instead, the trend in almost every case involved social media. Over half these cases involved individuals 25 or younger, and most troubling, a[ ]third involve kids that are 21 or under."[277]

Regardless of the political party in power at any given moment, the concept of national security has come to play a consistently central role in politics and governmental affairs in the twenty-first century.[278] As society and government alike recognize the growing threat posed by terrorists' use of social media, concerns surrounding the correlation between national security and FTO's effective manipulation of the internet have begun to play an increasingly central role in the national security conversation.[279]

---

273. *See* Tsesis, *supra* note 11, at 613. "Statutes regulating social media responsibility for inciteful messages posted by third parties raise First Amendment concerns about how to maintain national security while safeguarding free expression." *Id.* There needs to be a balance between the protection of free speech and information and the government's duty to counter terrorism. *Id.*

274. *See* discussion *infra* Sections V.A–B.

275. *See* discussion *supra* Section III.A.

276. *Justice Department Official: ISIS "Crowdsourced" Terrorism by Exploiting Social Media*, PBS (Dec. 12, 2015, 7:19 PM), https://www.pbs.org/newshour/show/justice-department-official-isis-crowdsourced-terrorism-by-exploiting-social-media.

277. *Id.* Carlin continued on to note that this trend has only come to fruition since the advent of social media. *Id.*

278. Zachary Leibowitz, *Terror on Your Timeline: Criminalizing Terrorist Incitement on Social Media Through Doctrinal Shift*, 86 FORDHAM L. REV. 795, 813 (2017). Legislative activity and exponential budget increases have been poured into fighting terrorism on a global scale. *Id.*

279. *See* Yigal Carmon & Steven Stalinsky, *Terrorist Use of U.S. Social Media Is a National Security Threat*, FORBES (Jan. 30, 2015, 1:36 PM), https://www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/#73d4ec144761. World leaders acknowledge that terrorists have grasped the power of social media and learned to capitalize on it. *Id.* Thus, solutions to future national security concerns inherently require addressing the dangers

The majority of social media platforms do not dispute this larger issue and even claim to provide some voluntary contribution to the fight against terrorism.[280] However, such methods are generally arbitrary in their approach, and while recent years have certainly seen an uptick of enforcement of such mechanisms by these private entities, this is far more motivated by public pressure than any type of moral compunction or legal requirement.[281] The danger here is that, when the momentary pressures of intense press coverage or public interest fade, so will the incentive of these companies to actively take part in limiting terrorists' use of their platforms.[282]

Moreover, even the best intended or well-thought-out plan for addressing terrorism use that may be implemented by the individual creators of one platform—no matter how brilliant or effective—cannot solve the larger issue.[283] Particularly in light of today's rapidly developing and ever-evolving world, a long-term, more uniform solution is needed to set a definitive standard for all social media platforms.[284] The social media sites of today are not the social media platforms of tomorrow, and the current attitude of

posed by social media and its use in terrorism. *Id.*; *see* Klein & Flinn, supra note 24, at 69–71. ("This use of the Internet 'permit[s] Islamist terrorist groups to maintain an active, pervasive, and amplified voice' that offsets intelligence and law enforcement successes. Commentators often criticize the tendency of these Internet platforms to 'robotically amplify the ISIS message.'" (quoting *Lieberman Calls on Google to Take Down Terrorist Content*, U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFF. (May 19, 2008)), https://www.hsgac.senate.gov/media/majoritymedia/lieberman-calls-on-google-to-take-down-terrorist-content; Berger, *supra* note 43.

280. *See* Emily Dreyfuss, *Facebook's Counterterrorism Playbook Comes into Focus*, WIRED (June 17, 2017, 7:00 AM), https://www.wired.com/story/facebook-counterterrorism/; Adam Satariano, *Twitter Suspends 300,000 Accounts Tied to Terrorism in 2017*, BLOOMBERG TECH. (Sept. 19, 2017, 7:57 AM), https://www.bloomberg.com/news/articles/2017-09-19/twitter-suspends-300-000-accounts-in-2017-for-terrorism-content.

281. *See* Sophia Cope, Jillian C. York & Jeremy Gillula, *Industry Efforts to Censor Pro-Terrorism Online Content Pose Risks to Free Speech*, ELECTRONIC FRONTIER FOUND. (July 12, 2017), https://www.eff.org/deeplinks/2017/07/industry-efforts-censor-pro-terrorism-online-content-pose-risks-free-speech. Threats by governments in the United States and Europe, coupled with the public concerns, have led social media companies to be more proactive in the fight on terror. *See, e.g.*, Satariano, *supra* note 280 (recognizing that Twitter's improvements in fighting terror came "under pressure from governments around the world").

282. *See* Anders Aslund, *Regulate Social Media—Just Like Other Media*, HILL (Oct. 5, 2017, 11:00 AM), http://thehill.com/opinion/national-security/354006-regulate-social-media-just-like-other-media ("Facebook and Twitter have already proven that they are unable to self-regulate. Congress needs to pick up the baton and legislate sensible rules for the regulation of social media.").

283. *Id.* Individual action creates no standard or broader sense of accountability. *Id.* To ensure that terrorists' use of social media sites actually decreases, there needs to be an external, objective, and minimum standard uniformly enforced. *See id.*

284. *See id.*

cooperation between social media platforms and the government is not guaranteed to continue.[285] Thus, to ensure national security and safeguard the future of counter-terrorism, there must be a means of holding these social media platforms accountable when they are *not* acting responsibly and do *not* choose an approach of proactivity—and there must be standards so that they know when they are falling short of their duty.[286] Imposing liability on social media companies as material supporters of terror is, in today's landscape, the most effective way to do just that.

B. Freedom of Speech

That said, however, First Amendment advocates often rise up in outrage at the idea that social media companies should face liability as contributors to terrorism.[287] "Statutes regulating social media responsibility for inciteful messages posted by third parties raise First Amendment concerns about how to maintain national security while still safeguarding free expression."[288]

It is a central tenant of American law that private speech is protected when people express unpopular views.[289] It is protected when people even advocate violent philosophical or religious doctrines.[290] Opponents of limiting the immunity of § 230 point to the significant impact that it would have on the enormous and ever-growing number of social media users.[291] The in-

285. Even currently, most social media companies do not consistently cooperate with the government. *See generally* April Glaser & Kurt Wagner, *Twitter Reminds Everyone It Won't Cooperate with Government or Police Surveillance*, RECODE (Nov. 22, 2016, 9:24 PM), https://www.recode.net/2016/11/22/13719876/twitter-surveillance-policy-dataminr-fbi.

286. See *infra* Part VI for a discussion of potential remedies and approaches to addressing this substantial problem.

287. *See* Lincoln Caplan, *Should Facebook and Twitter Be Regulated Under the First Amendment?*, WIRED (Oct. 11, 2017, 7:00 AM), https://www.wired.com/story/should-facebook-and-twitter-be-regulated-under-the-first-amendment/ ("[A]s it stands, the country's libertarian conception of free speech is allowing, and even ferociously feeding, an erosion of the democracy it is supposed to be essential in making work—and some government regulation of speech on social media may be required to save it.").

288. Tsesis, *supra* note 11, at 613.

289. *See* Caplan, *supra* note 287; Michelle Roter, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1401 (2017) (stating that the First Amendment has prohibited the federal government from "limit[ing] citizens' ability to express themselves based on the idea or message communicated through their expression" and the "right to speak freely is one of the most fervently protected rights . . . provided for in the Constitution").

290. *See id.*

291. Jacyln K. Haughom, *Combatting Terrorism in a Digital Age: First Amendment Implications*, FREEDOM F. INST. (Nov. 16, 2016), http://www.freedomforum.org/first-amendment-center/topics

ternet is frequently praised as a bastion of free speech, an equalizer enabling everyone to share their views, regardless of their background or monetary limitations.[292] It is true that the internet, at its best, is an embodiment of free speech principles and properly deserves a high degree of protection.[293] However, protecting free speech does not mean protecting threats of actual political violence.[294] As first established in *Brandenburg v. Ohio*, where the Court declined to give First Amendment protection to the speech of a Ku Klux Klan leader advocating violence against the government, First Amendment protection ends where advocacy of *responsive* violence begins.[295] Courts have repeatedly distinguished discussing unpopular views from furthering acts of violence.[296]

Protecting free speech does not mean permitting known supporters of ISIS, Hezbollah, or other terror organizations to capitalize on the services provided by these platforms to convert and educate killers and glorify the ideologically-motivated murder of innocents.[297] Fighting terrorism does not

/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/ ("As of April 2016, Facebook had 1,590 million active users, Twitter had 320 million active users, and Instagram had 400 million active users.").

292. *See* Dan Truong, *The Great Equalizer 2.0*, HUFF. POST (June. 27, 2015), https://www.huffingtonpost.com/dan-truong/the-great-equalizer-20_b_7157662.html (discussing how the internet is idyllically portrayed as a space of equality—and the inaccuracies underlying this view).

293. Haughom, *supra* note 291 ("Social media platforms embody the principles on which the First Amendment was built, as they provide 'an increasingly influential medium of communication' that 'facilitates unprecedented levels of expression and the exchange of ideas.' The Internet is a 'borderless medium,' that empowers users 'to evade governmental efforts to suppress hostile ideas,' by using social media as a mechanism to post the content of their choosing." (footnotes omitted) (quoting Aaron D. White, *Crossing the Electronic Border: Free Speech Protection for the International Internet*, 58 DEPAUL L. REV. 491, 492 (2009))); Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN ST. L . REV. 1005, 1012 (2015); Steven G. Gey, *Fear of Freedom: The New Speech Regulation in Cyberspace*, 8 TEX. J. WOMEN & L. 183, 185 (1999).

294. Tsesis, *supra* note 11, at 616 ("It is one thing when virtually independent parties use Twitter accounts or Facebook pages to articulate offensive or noxious ideas and a very different matter when those who post are coordinating with organizations like ISIS, Hezbollah, Hamas, or Al-Qaeda in an effort to invigorate and instruct persons to act on ideologically violent teachings. These are organizations that conspire with supporters to imperil innocents. When this activity becomes known to the digital intermediary, recalcitrant failure to take it down and report it to the proper law enforcement authorities entangles internet platforms with the terrorist activities.").

295. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (developing a two-part test regarding when speech could be properly regulated).

296. Haughom, *supra* note 291.

297. Tsesis, *supra* note 11, at 615–16. While mere correlation between speech and violence is not sufficient to create liability, when the speech "coerced or triggered the harmful acts," it is well-

have to come at the expense of maintaining free speech—and it should not.[298] However, neither should the effective application of national security be abrogated or threatened by protecting the non-existent right of terrorist actors to recruit, train, and communicate on a social media network.[299]

VI. RECOMMENDATIONS FOR THE FUTURE: FINDING WAYS TO HOLD SOCIAL MEDIA COMPANIES LIABLE WITHOUT COMPROMISING

The obstacles facing plaintiffs attempting to impose liability on social media companies who provide support to terrorists are large, and the policy concerns that must be navigated in doing so are significant.[300] However, the cost of *not* addressing this issue is far too great to even contemplate allowing the status quo to continue.[301] There are two major fronts on which changes are needed.[302] The first is in regard to judicial treatment of these cases.[303] The second is in regard to affirmative legislative action.[304]

A. Challenging Judicial Interpretation and Considering Alternative Theories of Responsibility

Section 230, as it has been applied by the lower courts, functionally serves as a road block, precluding any and all liability by social media sites for the activities on them.[305] However, this is an improper application of § 230.[306] The CDA's purpose, after all, was to protect good Samaritans who choose to censor content—not to provide a safe haven for those who *refuse*

established that liability is appropriate and does not infringe upon the protections of the First Amendment. *See* Christopher E. Campbell, *Murder Media—Does Media Incite Violence and Lose First Amendment Protection?*, 76 CHI.-KENT L. REV. 637, 668 (2000).

298. Caplan, *supra* note 287.

299. See *supra* Part II for a discussion of the uses of social media by terrorists.

300. *See supra* Parts III, IV.

301. *See* A.J. Willingham, *ISIS Has Mastered the Art of Creating Lone Wolves*, CNN (Mar. 23, 2017, 2:05 PM), https://www.cnn.com/2017/03/23/world/isis-lone-wolf-social-media-trnd/index.html ("Some of the most devastating attacks in the Western world as of late have been of the 'lone wolf' variety, including the shootings in Orlando and San Bernardino; and the truck attacks in Nice and Berlin. ISIS media regularly encourages these attacks and recommends locations and methods.").

302. *See* text accompanying *infra* notes 303–04.

303. *See infra* Section VI.A.

304. *See infra* Section VI.B.

305. Spivak, *supra* note 227.

306. *See Section 230 of the Communications Decency Act*, *supra* note 250.

to take action.[307] In addition—while the court's inappropriate application of § 230 has improperly precluded numerous plaintiffs from recovery—in most cases thus far, the failure of plaintiffs to successfully survive the § 230 immunity defense is grounded largely in the shortcomings of the plaintiffs' own cases.[308] Imposition of liability on social media companies for providing material support to FTOs is too often predicated on evidence of the particular posts on accounts controlled by FTOs and their affiliates.[309] However, the liability of social media companies does not come from the fact that these FTOs are posting photos of bloody machetes; while graphic and disturbing, such posts are not made by the social media companies and likely do fall within the scope of § 230 protection as it now stands.[310] Rather, the best theory for enforcing liability under the current law is grounded in the concept that these social media companies are knowingly providing a *service* to a known FTO.[311] This approach is "fundamentally different from the cases in which the courts rejected creative pleadings, in which they made clear that there was offending content" that constituted the central issue.[312] It is not about what is being posted; it is about the fact that social media companies are allowing FTOs and known FTO members to utilize social media and that service is enabling them to recruit, to convert, and to weaponize.[313]

In light of decisions reached so far, the best option for new plaintiffs seeking to move forward and recover against social media companies under the current law is to allege facts that clearly lay out how the provision of the services of the social media site to known FTOs and their supporters in some way proximately caused the resulting attack.[314] Only when such a suit is

307. *See CDA 230: Legislative History*, *supra* note 24.

308. *See supra* notes 262–63 and accompanying text.

309. *See, e.g.*, Fields v. Twitter, Inc., 881 F.3d 739, 750 (9th Cir. 2018). The account provisions theory bases liability on the actual accounts provided, not the content of them. *Id.*

310. *See* Roter, *supra* note 289, at 1381 (2017) (indicating that immunity protections provided under § 230 give ISPs "no legal duty to take down calls for acts of terror on their platforms, regardless of how graphic or incendiary the posts may be").

311. Wittes & Bedell, *supra* note 266.

312. *Id.*

313. *See Radicalization: Social Media and the Rise of Terrorism: Hearing Before the Subcomm. on Nat'l Sec. of the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 1–3 (2015) (statement of Ron DeSantis, Chairman of the Subcommittee on National Security) (indicating that terrorist organizations' use of social media platforms is "highly effective" for their "recruitment, mobilization, and financing efforts" in carrying out violent terrorist attacks).

314. Wittes & Bedell, *supra* note 266. This is an additional means of avoiding the concerns relating to the First Amendment. See *supra* Section V.B for a discussion of the public policy concerns

brought will a court finally provide a conclusive ruling on how the CDA must interact with this civil cause of action.[315] However, from both the perspective of policy and reasonableness, § 230 should not serve as a bar to liability when social media entities knowingly service terrorists.[316]

Some have compared the attempt to hold social media companies liable with the recent—and successful—push to find liability for banks that provide services to known terrorist actors.[317] For instance, in the groundbreaking *Linde v. Arab Bank* decision, the Eastern District of New York found a foreign bank liable for handling transfers and payments of Hamas members.[318] Similar to the discussion now surrounding social media liability, the plaintiffs in that case held the burden of proving that Hamas conducted the connected attacks and that the bank's support of the acts were both foreseeable and a proximate cause of them.[319] Although currently under review, that decision paved the way for holding banks liable when they provide material support to terror organizations, even if they are not breaking a single banking law in the process.[320] The similarities to this situation are difficult to ignore, and—just as in the banking case—one strong case is all that is necessary to open the flood gates and show that cases against social media companies can—and should—be brought.[321] In the judicial arena, plaintiffs and attorneys need to exercise patience going forward.[322] The right case, brought with facts clearly showing the causal relationship between usage of the service of a social media platform and a subsequent attack, could help to reverse the tide of judicial sentiment and begin chipping away at § 230's inappropriate protection of social media companies' enabling of terrorists;

---

related to the First Amendment.

315. *See supra* notes 263–70 and accompanying text. To date, no case has both alleged strong facts in support of causation and provided strong arguments regarding the CDA.

316. *See generally* Wittes & Bedell, *supra* note 266.

317. *See* Stephanie Clifford, *Arab Bank Liable for Supporting Terrorist Efforts, Jury Finds*, N.Y. TIMES (Sept. 22, 2014), https://www.nytimes.com/2014/09/23/nyregion/arab-bank-found-guilty-of-supporting-terrorist.html.

318. Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287 (E.D.N.Y. 2015), *vacated*, 882 F.3d 314 (2d Cir. 2018).

319. *See* Clifford, *supra* note 317 (commenting on the high burden of proof).

320. *Id.* "The verdict is expected to have a strong impact on similar legal efforts to hold financial institutions responsible for wrongdoing by their clients, even if the institutions followed banking rules, and could be seen as a deterrent for banks that conduct business in violent areas." *Id.*

321. *See id.*

322. *See* Wittes, *supra* note 259 (discussing the increasing proliferation of material support litigation against social media companies that would likely fail to demonstrate causation, even if it did survive § 230 immunity).

however, the more losing cases that are brought, the higher the precedential burden, and the more entrenched the courts' sentiments in relation to the CDA will become.[323]

B. Legislative Changes

That said, while the action and interpretation by the judiciary may certainly play a significant role in fostering a future where social media companies are held accountable for their actions, Congress also must act, either by revising § 230 or amending the definition of material support—or both—and create a statute to address the need for responsibility on the part of social media companies in clear and unambiguous terms.[324]

First, Congress could revise § 230.[325] Ideally, any revision of § 230 should focus on narrowing the scope of its protections, including creating a specific exception exempting social media providers from protection.[326] This could take the form of limiting protection to ISPs who take "reasonable steps to prevent or address unlawful use of its services," which would limit social media companies' ability to use § 230 as a shield to those instances in which it can be demonstrated that they have taken effective and active steps to avoid supporting terrorism or any other illegal activity.[327] At a minimum, if the remainder of the provision is left untouched, a revision of § 230 could eliminate protection for social media sites who currently use this provision as a hiding place to enable terrorism by creating a specific anti-terror exception.[328] Given the growing consensus that a change is needed in § 230, this

323. *See generally* John M. Walker, Jr., *The Role of Precedent in the United States: How Do Precedents Lose Their Binding Effect?*, CHINA GUIDING CASES PROJECT (Feb. 29, 2016), https://cgc.law.stanford.edu/wp-content/uploads/sites/2/2016/02/Commentary-15-English.pdf (noting that the more entrenched and extensive the persuasive precedential case law, the more difficult it will be to overcome it).

324. *See infra* text accompanying notes 325–48.

325. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 418–19 (2017).

326. *Id.* at 408 ("[T]he broad construction of the CDA's immunity provision adopted by the courts has produced an immunity from liability far more sweeping than anything the law's words, context, and history support.").

327. *Id.* at 419.

328. *Id.* As a matter of policy and legislative efficiency, a broader revision would be appropriate to address not only the issue of terrorism but similar social media-related challenges that consistently face the same barrier in litigation. *See* Keller, *supra* note 21. In general, the current "environment of perfect impunity for intermediaries that facilitate online abuse is not an obvious win for free speech if the result is that the harassers speak unhindered and the harassed retreat in fear offline." Citron & Wittes, *supra* note 325, at 420.

is likely the most efficient approach, particularly given that, with the online trafficking bill passed in early 2018, Congress already demonstrated a willingness to abrogate the section's broad immunity provision when the evolving nature of the internet necessitates it.[329]

That said, social media companies are particularly opposed to amending § 230 because they fear the larger impact it may have on them outside of the anti-terror context.[330] Accordingly, to avoid further conflict with the tech giants of Silicon Valley, Congress could choose to approach the issue by amending the definition of material support used in the material support provisions.[331] Specifically, adding language that specifies provision of a social media platform constitutes a service within the definition of material support would change the analysis and redefine the trajectory of this line of litigation in much the same way as altering § 230.[332] Under such a revision, knowingly providing a social media platform to a terrorist would be independently sufficient to constitute a violation of § 2339B, and all the ambiguity and complications surrounding causation and immunity currently muddling such litigation would be effectively moot.[333] Instead, the lines of liability would be clearly defined.[334] Social media companies would know when they are crossing them, and plaintiffs would know when they can recover for violations.[335] The easiest way to enforce liability would be to place the emphasis of new litigation on the plaintiffs, requiring them to show that the social media company from whom they seek recovery either knew or should have known that the account in question belonged to an FTO or its affiliate.[336]

This, of course, raises an even greater underlying question: what circumstances establish that a social media company "should have known?" This issue goes hand-in-hand with recognition of the important reality that, while it is key to be able to hold social media companies liable when they do

329. *See* Keller, *supra* note 21.

330. *See* April Glaser, *The Law That Let Silicon Valley Stay Clueless*, SLATE (Nov. 16, 2017, 1:55 PM), http://www.slate.com/articles/technology/future_tense/2017/11/the_law_that_let_silicon_valley_stay_clueless_made_the_internet_we_have.html (discussing how the internet under § 230 has "morph[ed] into [an] overgrown safe haven[]").

331. *See* Schwartz, *supra* note 172, at 1212–16.

332. *See id.*

333. *Id.* at 1213 (acknowledging that "by merely knowingly providing a social medial platform, a social medial company would violate section 2339B's plain language" under this theory).

334. *See id.*

335. *Id.* at 1214–15. In addition, regardless of whether Congress passed an amendment to the CDA, this would independently address the problem by ensuring that the liability is predicated on the account provision, not the content posted. *Id.* at 1214.

336. *See* discussion *supra* Section III.B.

provide material support to terrorists, the ultimate goal is to prevent the situations that give rise to this type of liability in the first place.[337] With the "exponential increase in terror activity and dissemination of terrorist-related information and propaganda and the proliferation of Internet connectivity . . . online facilitation will only become more frequent."[338] Thus, Congress must pursue a line of legislation that imposes an affirmative duty on social media companies, not only to take responsibility when terrorist activity on their sites is brought to their attention, but to take action to detect and address such accounts and individuals *before* their presence destroys the life of an impressionable teenager or leads to a mass murder.[339] Failure of a social media company to meet the basic affirmative monitoring and action requirements would, in turn, be evidence that the social media company's actions satisfied the necessary *mens rea* for liability.[340] While many social media companies often do elect to self-regulate and play an active role in removing terrorist material from their websites, there are also times when they do not.[341] Creating legislation which uniformly requires some level of

337. *See* Klein & Flinn, *supra* note 24, at 73 ("It is no doubt useful to discover individual terror recruits, but the aims of U.S. counterterrorism online stretch far beyond identification—they include finding recruits, terminating wide terror conspiracy operations, and shutting down the communications infrastructure enabling terror cells.").

338. *Id.*

339. *See id.* at 112 (proposing solutions that "offer a solid framework for catching foreign and domestic individuals intent on assisting foreign terrorist organizations or attacking themselves before they strike"). Opponents to regulation assert that there would be a significant cost to the social media companies. *See id.* at 98. However, the national security issues at stake are sufficient to justify such regulation regardless of the cost because the reality is that most social media companies already *are* increasing their affirmative action under public pressure, and therefore, the cost increase to the majority of these entities will likely be insubstantial. *See* Reuters, *Facebook, YouTube, Twitter, and Microsoft Join to Fight Against Terrorist Content*, CNBC (June 26, 2017, 2:21 PM), https://www.cnbc.com/2017/06/26/social-media-companies-join-to-fight-against-terrorist-content.html.

340. *See* Klein & Flinn, *supra* note 24, at 69–70 ("As long as these sites continue to openly provide fora for the distribution of terrorist material, each one of them provides material support to an FTO, which, if done knowingly, would be in direct contravention of 18 U.S.C. § 2339B. These social media sites must be encouraged to discover offending posts and report them to federal law enforcement authorities to avoid what on a practical level constitutes complicity with terrorist organizations."). Even major players in the social media industry, including Mark Zuckerberg, acknowledge that some regulation is likely necessary in the changing internet landscape. April Glaser, *How to Regulate Facebook*, SLATE (Mar. 22, 2018, 8:00 PM), https://slate.com/technology/2018/03/mark-zuckerberg-says-hes-open-to-regulation-what-could-it-look-like.html.

341. *See, e.g.*, Satariano, *supra* note 280. Twitter suspended 300,000 accounts of terrorists in one year. *Id.* Facebook is developing artificial intelligence technology to fight terrorism on its platforms. Dreyfuss, *supra* note 280. Regardless, there is a general consensus that social media companies are not doing enough. Joe Watts, *Theresa May Calls on Social Media Companies to 'Step Up'*

affirmative action on the part of social media companies would ensure a constant standard of excellence, mandating the "minimum" that an organization can choose to do.[342]

Other nations have already begun to go down this path, requiring increased responsibility of social media companies.[343] In January 2018, Germany passed a new law requiring social media companies to address all reported instances of hate speech—including "terrorist incitement or propaganda"—within forty-eight hours of them being reported.[344] The European Union is also considering additional proposals for addressing terrorist speech on social media, including seriously contemplating the imposition of affirmative burdens for these platforms to actively address these issues.[345] In February 2018, the European Commission instituted a "one-hour rule," requiring that terror-related content be removed within an hour of it being posted.[346] In the United Kingdom, Security Minister Ben Wallace is currently advocating for a tax-based approach on technology firms, to counter the rising cost of combatting online terrorism if these organizations do not self-regulate in an effective manner.[347] While it remains to be seen which—if

---

and Tackle Online Abuse, INDEP. (Feb. 5, 2018, 11:30 PM), https://www.independent.co.uk/news/uk/politics/theresa-may-online-abuse-social-media-suffragette-jeremy-corbyn-a8196126.html. British Prime Minister Theresa May recently noted, "The social media companies themselves must now step up and set out how they will respond." *Id.*

342. *Cf.* Natasha Lomas, *Social Media Handed "One-Hour Rule" for Terrorist Takedowns in Europe*, TECHCRUNCH, https://techcrunch.com/2018/03/02/social-media-handed-one-hour-rule-for-terrorist-takedowns-in-europe/ (last visited Oct. 8, 2018).

343. *See Europe Could Follow Germany in Social Media Hate Laws*, CONNEXION (July 4, 2017), https://www.connexionfrance.com/French-news/Europe-could-follow-Germany-in-social-media-hate-laws.

344. *Id.*

345. *Id.*; *see also* Hamza Shaban, *Facebook Braces for New E.U. Privacy Laws*, WASH. POST (Jan. 29, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/29/facebook-braces-for-new-e-u-privacy-law/ (discussing new privacy laws in the European Union and their impact on social media).

> Where the provision of videos forms an "essential part" of the services provided by a social media company, they will have to take measures to block videos with hate speech, incitement to hatred and content justifying terrorism from their platforms. This could include establishing mechanisms for users to flag such content.

Julia Fioretti, *EU States Approves Plans to Make Social Media Firms Tackle Hate Speech*, REUTERS (May 23, 2017, 7:54 AM), https://www.reuters.com/article/us-eu-hatespeech-socialmedia-idUSKBN18J25C.

346. Lomas, *supra* note 342.

347. Natasha Lomas, *UK Eyeing 'Extremism' Tax on Social Media Giants*, TECHCRUNCH, https://techcrunch.com/2018/01/02/uk-eyeing-extremism-tax-on-social-media-giants/ (last visited Oct. 8, 2018). As UK Security Minister Ben Wallace noted, "We should stop pretending that because they sit on beanbags in T-shirts they are not ruthless profiteers. They will ruthlessly sell our

any—of these routes is the best way to proactively fight future attacks and prevent exploitation of social media by terrorists, there is no question that allowing social media giants to go unchallenged and unregulated is going to ensure that terrorists' use of social media continues to rise.[348]

VII. CONCLUSION

British statesman Edmund Burke once said, "The only thing necessary for the triumph of evil is for good men to do nothing."[349] That certainly rings true here.[350] Terrorist attacks by individual actors are on the rise in the western world.[351] As a society, it can be difficult to understand the *why* behind these horrendous and senseless massacres.[352] Sometimes, when the attacks come at the hands of this country's own soldiers and citizens, attempting to understand the *who* behind these attacks can leave even deeper scars.[353] However, in the midst of the unknown and unpredictable, there is one common denominator within these attacks, the *how* that ties them all together: social media.[354] From recruiting idealistic American teens to teaching bomb-building for dummies, terrorist organizations have recognized the value of these platforms and capitalized on them—often, with startlingly

details to loans and soft-porn companies but not give it to our democratically elected government." *Id.*

348. *See id.* Some major social media companies have taken significant steps to attempt to curb use of social media by terrorists. *See* Reuters, *supra* note 339. While much can be learned from the actions of European nations, because the level of protection for free speech is higher in the United States, a somewhat different approach from that of Europe may be necessary to successfully regulate social media platforms without abrogating free speech. *See* discussion *supra* Section V.B.

349. Robert F. Blomquist, *In Search of Themis: Toward the Meaning of the Ideal Legislator - Senator Edmund S. Muskie and the Early Development of Modern American Environmental Law, 1965-1968*, 28 WM. & MARY ENVTL. L. & POL'Y REV. 539, 648 (2004).

350. See discussion *supra* Part II regarding how use of social media by terrorists has grown exponentially over the past few years.

351. *See* Daniel L. Byman, *Can Lone Wolves Be Stopped?*, BROOKINGS (Mar. 15, 2017), https://www.brookings.edu/blog/markaz/2017/03/15/can-lone-wolves-be-stopped/.

352. Natasha Bertrand, *A Former FBI Agent Revealed the Motivations Behind 'Lone Wolf' Terrorists, and They're Terrifying*, BUS. INSIDERS (Feb. 25, 2015, 4:31 PM), http://www.businessinsider.com/a-new-study-sheds-light-on-what-motivates-a-lone-wolf-terrorist-2015-2 (discussing the complexity of motives underlying lone-wolf terrorism).

353. *See generally* Mockaitis, *supra* note 54 ("The lone wolves who have hit American targets in the past few years were either born in the U.S. or immigrated as children.").

354. Willingham, *supra* note 301. "With the rise of online or remote radicalization, would-be extremists don't ever need to make contact with ISIS figures, or even deeply understand their motives, to carry out the next big attack." *Id.*

successful results.[355] That is why it has become imperative, in the interest of national security, the protection of innocent lives, and the furtherance of counter-terror operations, that measures be taken to change this.[356]

Change should begin with ensuring that the laws that currently exist in the United States are being properly interpreted to allow for liability when social media companies are knowingly providing material support to terror actors.[357] By focusing on the provision of a service and recognizing that speech which incites violence is not constitutionally protected, such liability can be properly imposed without any infringement of the freedom of speech intended by the First Amendment.[358] What it will do, however, is significantly further the national interest in protecting national security and innocent lives.[359] Failure to take action when a known threat of terrorists' use of social media has been identified—particularly where there are easily identifiable means and methods to attempt to combat it—is either indicative of laziness or pure, unconscionable indifference—the type of indifference that leads to the loss of more life and greater harms.[360] The courts and Congress, together, must lead the charge to change this dynamic here in the United States.[361] While there is much that needs to be done in addressing this issue, it is comforting to recognize that there is much that *can* be done, and moving forward, this needs to be the attitude and focus of litigation and legislation alike.[362] There is no way to turn back the clock. There is no way to go back and stop the Boston bombers from learning to make those bombs on a video[363] or change the past and stop American youths recruited online from running to Syria to fight alongside ISIS.[364] There can be no going back, but there is time to go forward and begin imposing the material support provisions against social media companies in order to ensure that social media

355. See *supra* Part II for a discussion of the use of social media by terrorists.

356. *See* Willingham, *supra* note 301.

357. *See supra* Parts III–IV.

358. *See supra* Section V.B.

359. *See supra* Section V.A.

360. *See supra* Part VI.

361. *See supra* Part VI.

362. *See supra* Part VI.

363. Azmat Khan, *The Magazine That "Inspired" the Boston Bombers*, PBS (Apr. 30, 2013), https://www.pbs.org/wgbh/frontline/article/the-magazine-that-inspired-the-boston-bombers/.

364. *See, e.g.*, Kevin Sullivan, *Three American Teens, Recruited Online, Are Caught Trying to Join the Islamic State*, WASH. POST (Dec. 8, 2014), https://www.washingtonpost.com/world/national-security/three-american-teens-recruited-online-are-caught-trying-to-join-the-islamic-state/2014/12/08/8022e6c4-7afb-11e4-84d4-7c896b90abdc_story.html.

does not remain a deadly tool in the arsenal of terrorism.

Anna Elisabeth Jayne Goodman*

* J.D. Candidate, Pepperdine University School of Law; B.A. in Communication Studies, Union University. Thank you to my entire family for their support and encouragement throughout my law school career, including both my parents and Steve and Deb McDowell, and especially to my mother for her consistent support and encouragement. Thank you also to all those I've been privileged to work with on the *Pepperdine Law Review* and their outstanding work in the process of editing this Comment.