Hofstra Law Review

Volume 45 | Issue 4 Article 14

5-1-2017

With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media

Michelle Roter

NOTE

WITH GREAT POWER COMES GREAT RESPONSIBILITY: IMPOSING A "DUTY TO TAKE DOWN" TERRORIST INCITEMENT ON SOCIAL MEDIA

I. INTRODUCTION

James Foley was a dedicated American journalist who often risked his life for the sake of reporting, putting himself in the midst of dangerous conflicts to raise awareness of serious humanitarian crises that plague the global community.[1] In 2012, while investigating a story on the rising turmoil in Syria, Foley was captured for the second time in his career as a front-line journalist.[2] News of his disappearance reached the mainstream media in 2013 when his family created a media campaign pleading for his release.[3] However, all hope for Foley's return immediately came to a halt on August 19, 2014, when the Islamic State of Iraq and Syria, more commonly known as ISIS, released a video graphically depicting a murder that confirmed the fears of his family and the American public.[4]

---

1. *See The Biography and Timeline of American Journalist James Foley*, NEWSLAB, http://newslab.us/article/the-biography-and-timeline-of-american-journalist-james-foley (last visited Aug. 1, 2017).

2. *Id.* Foley had previously been captured in Libya while reporting on the civil uprising against Muammar Gaddafi in 2011. *Id.*

3. *Id.* Foley's family did not initially publicize his disappearance pursuant to suggestions from security experts who were still investigating which group was responsible for his capture. Andrew Beaujon, *James Foley Likely 'Being Held With One or More Western Journalists' in Syria*, POYNTER (May 3, 2013), http://www.poynter.org/2013/james-foley-likely-being-held-with-one-or-more-western-journalists-in-syria/212510.

4. Zack Beauchamp, *18 Things About ISIS You Need to Know, ISIS Captured and Executed James Foley and Steven Sotloff, Two American Journalists*, VOX (Nov. 17, 2015, 10:25 AM), http://www.vox.com/cards/things-about-isis-you-need-to-know/james-foley-isis; Manuel Roig-Franzia, *James Foley Was a Journalist Who Had to Be There*, WASH. POST (Aug. 20, 2014), https://www.washingtonpost.com/lifestyle/style/2014/08/20/1de47c42-28ae-11e4-958c-268a320a60ce_story.html.

Originally posted to YouTube, but later shared on many other social media platforms,[5] the video was titled "A Message to America" and started with a clip of former President Obama discussing his plan to launch airstrikes against forces belonging to ISIS.[6] A masked militant dressed in all black then appeared next to Foley, who was positioned on his knees in an orange jumpsuit.[7] After Foley was given a chance to say some final words, the terrorist gruesomely beheaded him.[8] There is no doubt that the purpose of this video was to influence American foreign policy as the masked murderer warned the Obama Administration that its continued military presence in Syria "will result in the bloodshed of [the American] people."[9] However, many of those who are familiar with the organization believe that ISIS had another objective in mind—to establish itself as a leader in the global jihadist movement in order to earn support and respect from other terrorist groups and sympathizers around the world.[10] YouTube removed the video within hours, but terrorists continue to use social media as a means to forcibly insert themselves into the mainstream news.[11]

The world has benefitted from the advent of Facebook, YouTube, Twitter, and other social media platforms that have allowed for vast communication on a global scale.[12] However, these Internet platforms have also served as a medium for terrorist groups to devise and inspire acts of terror that have put the lives of many in jeopardy.[13] In recent

---

5. Brian Stelter, *James Foley Beheading Video: Would You Watch It?*, CNN (Aug. 21, 2014, 1:21 PM), http://www.cnn.com/2014/08/20/us/isis-beheading-social-media.

6. Hayes Brown, *The Social Media Strategy Behind the Brutal Beheading of an American Journalist*, THINKPROGRESS (Aug. 20, 2014), https://thinkprogress.org/the-social-media-strategy-behind-the-brutal-beheading-of-an-american-journalist-401d9bdc7169#.iojkd5eh9.

7. Lee Ferran & Rym Momtaz, *Video Appears to Show Beheading of Journalist James Foley, who Went Missing in Syria*, ABC NEWS (Aug. 19, 2014, 5:55 PM), http://abcnews.go.com/Blotter/james-foley-video-appears-show-beheading-journalist-missing/story?id=25043593.

8. *Id.*

9. Brown, *supra* note 6.

10. *See id.* (quoting counterterrorism expert J.M. Berger, claiming that ISIS "may also hope to win support and loyalty from others in the global jihadist community").

11. *See* Stelter, *supra* note 5; Gabriel Weimann, *New Terrorism and New Media*, WILSON INT'L CTR. FOR SCHOLARS 1-3 (2014), https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf.

12. *See* Alejandra Guzman & Farida Vis, *6 Ways Social Media Is Changing the World*, WORLD ECON. F. (Apr. 7, 2016), https://www.weforum.org/agenda/2016/04/6-ways-social-media-is-changing-the-world.

13. *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media: Hearing Before the Subcomm. on Terrorism, Nonproliferation, and Trade of the H.R. Comm. on Foreign Affairs*, 114th Cong. 10 (2015) [hereinafter *Hearings on Evolution of Terrorist Propaganda*] (testimony of Mark Wallace, Chief Executive Officer, Counter Extremism Project) (citing a Wilson Center report that found 90% of terrorists utilize social media networking services to promote terrorism online).

years, companies like Facebook and Twitter have found themselves subject to lawsuits brought by victims of terror and their families for their alleged failure to curb the dissemination of material inciting terrorist activity.[14] These cases have gained little traction and tend to be quickly dismissed due to the automatic protection granted to social media providers under section 230 of the Communications Decency Act of 1996 ("CDA"), an Act that provides a safe harbor to any Internet Service Provider ("ISP") for content posted by third-party users.[15] Unlike content containing child pornography or copyright infringement, ISPs currently have no legal duty to take down calls for acts of terror on their platforms, regardless of how graphic or incendiary the posts may be.[16]

While many of these companies explicitly state in their "Terms of Service" that posts promoting violence, terrorist acts, or both, are prohibited, their efforts to remove these posts are in no way compulsory and their willingness to cooperate tends to vary between platforms.[17] Those primarily concerned with national security interests urge for greater surveillance of terrorist activity on social media and for more transparency on the current procedures used to remove the unwanted content.[18] However, skeptics often express fear that greater censorship would infringe on one's constitutionally protected right to freedom of speech.[19] Due to a lack of consensus as to what constitutes terrorist

---

14. *See, e.g.*, David Z. Morris, *Lawsuit Claims Twitter, Facebook, Google Liable for Terrorism*, FORTUNE (June 18, 2016), http://fortune.com/2016/06/18/lawsuit-tech-giants-terrorism; Abigail Tracy, *Facebook's $1 Billion Terrorism Lawsuit Points to a Huge Problem for Silicon Valley*, VANITY FAIR: HIVE (July 12, 2016, 9:04 AM), http://www.vanityfair.com/news/2016/07/facebook-billion-dollar-terrorism-lawsuit.

15. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.); Tracy, *supra* note 14.

16. Ellen Nakashima, *There's a New Tool to Take Down Terrorism Images Online. But Social-Media Companies Are Wary of It.*, WASH. POST (June 21, 2016), https://www.washingtonpost.com/world/national-security/new-tool-to-take-down-terrorism-images-online-spurs-debate-on-what-constitutes-extremist-content/2016/06/20/0ca4f73a-3492-11e6-8758-d58e76e11b12_story.html; *see also* MICHAEL L. RUSTAD & THOMAS H. KOENIG, SOFTWARE LICENSING, CLOUD COMPUTING AGREEMENTS, OPEN SOURCE, & INTERNET TERMS OF USE § 9.08 (2016).

17. *See* Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51, 87-88 (2015); *Community Standards, Dangerous Organizations*, FACEBOOK, https://m.facebook.com/communitystandards/helping-to-keep-you-safe (last visited Aug. 1, 2017); *The Twitter Rules*, TWITTER, https://support.twitter.com/articles/18311 (last visited Aug. 1, 2017); *YouTube Community Guidelines, Violent or Graphic Content*, YOUTUBE, https://support.google.com/youtube/answer/2802008 (last visited Aug. 1, 2017).

18. *See Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 42-45 (statement of J.M. Berger, Nonresident Fellow, Brookings Institution).

19. *See* Jenna McLaughlin, *Twitter Is Not at War with ISIS. Here's Why*, MOTHER JONES (Nov. 18, 2014, 7:30 AM), http://www.motherjones.com/politics/2014/11/twitter-isis-war-ban-speech (quoting a Twitter employee who stated "[o]ne man's terrorist is another man's freedom

incitement, social media platforms trying to curtail this increasingly more dangerous use of their services are often left in a position that they are ill-suited to handle, having to balance conflicting interests of free speech and national security.[20]

Amending the CDA to no longer provide complete immunity to ISPs may help incentivize these companies to continually manage the promotion of terrorist activity on their platforms.[21] By imposing a "duty to take down" the material upon notification of its inciting nature, based on the duty promulgated in the Digital Millennium Copyright Act ("DMCA"), these social media networks would be legally required to comply with takedown requests, and would be subject to civil liability if they fail to do so.[22] The imposition of this duty would hopefully cause social media companies to remove incendiary posts at rates similar to those that infringe on a copyright owner's use of her intellectual property.[23] However, social media giants cannot be expected to manage terrorist activity on their own and therefore require the help of the federal government to provide a more concrete definition as to what constitutes prohibited forms of terrorist incitement so that the lines of free speech and hate speech are no longer blurred.[24]

This Note begins by examining the history of the CDA, focusing on its purpose and the automatic protection it provides to ISPs under section 230.[25] It then discusses the rise of terrorism and its strong connection with social networking services, resulting in the growth of homegrown terrorism in the United States.[26] Part III concentrates on the issues that arise due to section 230's grant of immunity from liability, including the almost immediate dismissal of cases against ISPs that have allowed inciting material to remain on platforms, as well as the shortcomings in relying on social media companies to voluntarily monitor terrorist incitement themselves.[27] Part III also examines how other countries have successfully imposed legal obligations directing social media companies to regulate content in accordance with their specific standards and points

---

fighter").

20. Nakashima, *supra* note 16.

21. *See* Ira Steven Nathenson, *Super-Intermediaries, Code, Human Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 19, 110-12 (2013) (contrasting ISPs' lackluster efforts to manage defamatory content on their platforms due to section 230's grant of automatic immunity to ISPs' stringent removal of copyright infringing material as a result of the DMCA's notice-and-takedown regime).

22. *See* 17 U.S.C. § 512(c)(1) (2012); *see also infra* Part IV.

23. *See Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 63 (statement of Evan Kohlmann, Chief Information Officer, Flashpoint Partners).

24. *See id.* at 64-66.

25. *See infra* Part II.A.

26. *See infra* Part II.B–C.

27. *See infra* Part III.A–B.

out the unique limitations on the American government because of the country's sensitivity towards First Amendment infringement and its aversion to censorship.[28] Finally, Part IV proposes an amendment to the CDA that will impose on ISPs a duty to take down inciting material upon notification of its terroristic purposes, but will also seek to define terrorist incitement that does not deserve First Amendment protections.[29]

II. THE COMMUNICATIONS DECENCY ACT, THE RISE OF TERRORISM ON SOCIAL MEDIA, AND ITS IMPLICATIONS ON U.S. POLICY

When the CDA was created, the world was a different place—the Internet age had just begun and global terrorism was not nearly as much of a threat as it is in the modern day.[30] Subpart A discusses the history and relevant provisions of the CDA, while Subpart B highlights the simultaneous rise of social media and new terrorism.[31] Lastly, Subpart C summarizes the rise of homegrown terrorism in the United States and the federal government's recent response to address such noxious use of social media services.[32]

A. Communication Decency Act & Section 230's Grant of Automatic Immunity to Internet Service Providers

During a period often referred to as "the Great Internet Sex Panic of 1995,"[33] Congress introduced the CDA[34] in an effort to regulate the vast amount of obscene and pornographic material on the Internet.[35] As a direct response to the controversial *Stratton Oakmont* decision,[36] in

28. *See infra* Part III.C.

29. *See infra* Part IV.

30. The CDA was passed during a period when the Internet was "rapidly developing." 47 U.S.C. § 230(a)(1) (2012); *see also* Jesper Falkheimer, *Digital Media and New Terrorism*, *in* STRATEGIC COMMUNICATION, SOCIAL MEDIA, AND DEMOCRACY: THE CHALLENGE OF THE DIGITAL NATURALS 146-47 (W. Timothy Coombs et al. eds., 2016).

31. *See infra* Part II.A–B.

32. *See infra* Part II.C.

33. Wendy Hui Kyong Chun, *Screening Pornography*, *in* PUBLIC CULTURE DIVERSITY, DEMOCRACY, AND COMMUNITY IN THE UNITED STATES 143-44 (Marguerite S. Shaffer ed., 2008).

34. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.); William A. Sodeman, *Communications Decency Act (CDA)*, ENCYCLOPEDIA BRITANNICA (1996), https://www.britannica.com/topic/Communications-Decency-Act.

35. *See* Chun, *supra* note 33; Paul Ehrlich, *Communications Decency Act § 230*, 17 BERKLEY TECH. L.J. 401, 404-06 (2002); *CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history (last visited Aug. 1, 2017).

36. Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act of 1996, 47 U.S.C. § 230, *as recognized in* Shiamili v. Real Estate Grp. of N.Y., 952 N.E.2d 1011, 1016 (N.Y. 2011).

which an online service provider was deemed to have acted as a "publisher" of material posted by a third-party user due to its failed attempts to regulate the objectionable content,[37] Congress proposed a safe harbor to protect ISPs.[38] Legislators feared that punishing ISPs for inadequately trying to manage user content would cause providers to cease their efforts and remain idle when faced with content that clearly should be removed to shield themselves from liability.[39] In the hopes of incentivizing good-faith effort on the part of ISPs to create a "family-friendly" cyberspace, the "Good Samaritan" provision of section 230 was born.[40] After the revised bill passed through both houses of Congress, former President Clinton signed the CDA into action on February 8, 1996.[41]

In the landmark case *Reno v. ACLU*,[42] the Supreme Court invalidated many of the CDA's original provisions on the basis of First Amendment violations.[43] As soon as the CDA was implemented, twenty plaintiffs filed suit against the Attorney General of the United States, claiming that the anti-obscenity provisions of the CDA were violative of free speech and therefore unconstitutional.[44] A few weeks later, twenty-seven additional plaintiffs, backed by the ACLU, filed a separate suit also challenging the constitutionality of CDA provisions, and the two cases were consolidated upon the Supreme Court's grant of certiorari.[45] In an effort to protect the sanctity of the First Amendment, many of the provisions were nullified for vagueness.[46] The Court specifically rejected the provisions in question because they were content-based regulations of speech, which have traditionally been rendered unacceptable in the nation's First Amendment jurisprudence.[47] Despite the Court's intense

37. Fair Hous. Council v. Roommates.com, L.L.C., 521 F.3d 1157, 1163 (9th Cir. 2008) ("One of the specific purposes of [section 230] is to overrule [*Stratton Oakmont*] and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material."); *Stratton Oakmont*, 1995 WL 323710, at *4 (holding that defendant ISP acted as a "publisher" of third-party content for overlooking questionable content on its computer bulletin boards despite the company's good faith efforts to remove such material).

38. *CDA 230: Legislative History*, *supra* note 35 (discussing the Cox-Wyden Amendment).

39. *See* Zeran v. Am. Online, Inc., 958 F. Supp. 1124, 1134-35 (E.D. Va. 1997).

40. *Fair Hous. Council*, 521 F.3d at 1163; Nathenson, *supra* note 21, at 110-11.

41. ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230/legislative-history/timeline (last visited Aug. 1, 2017); *Legislative History*, *supra* note 35.

42. 521 U.S. 844 (1997).

43. *Id.* at 885; Ehrlich, *supra* note 35, at 401-02.

44. *Reno*, 521 U.S. at 861.

45. *Id.* at 861-62.

46. *Id.* at 870 ("[T]he many ambiguities concerning the scope of [the CDA's] coverage render it problematic for purposes of the First Amendment.").

47. *Id.* at 871; Daphne Barak-Erez & David Scharia, *Freedom of Speech, Support for*

scrutiny of the CDA, section 230 remained in place and has since been consistently interpreted to grant automatic immunity to ISPs for both publishing and distribution liabilities.[48]

An ISP is defined as "a business or other organization that offers Internet access, typically for a fee."[49] Although social media platforms like Facebook, Twitter, and YouTube did not exist at the time of section 230's inception, they do qualify as ISPs in that they often provide online social networking services to their users, though free of charge.[50] In order to qualify for immunity under section 230, an ISP must satisfy all elements of a three-pronged test.[51] A plaintiff's claim is barred if (1) the defendant is an ISP; (2) the content in question was posted by a third-party user or "another content provider"; and (3) the plaintiff's claim seeks to hold the defendant accountable as "publisher or speaker" of that content.[52]

Section 230's statutory purpose was recently discussed in a California case, in which the court noted that Congress sought to "offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and a myriad of avenues for intellectual activity."[53] It has allowed for virtual freedom for its users on cyberspace and has been strongly revered as "the most important law protecting speech" for many civil liberties advocates.[54] However, section 230 has more recently been characterized as a carrot without a stick, in that it was enacted to encourage ISPs to monitor obscene content on their websites without fear of liability, but has actually perpetuated ISP inaction due to a lack of any obligation.[55]

Terrorism, and the Challenge of Global Constitutional Law, 2 HARV. NAT'L SEC. J. 1, 14-16 (2011); *see infra* Part III.C.

48. *See* Ehrlich, *supra* note 35, at 406-08.

49. *Internet Service Provider*, BLACK'S LAW DICTIONARY (10th ed. 2014).

50. *See* Tom Johansmeyer, *Social Media Is Free: Social Media Marketing Is Not*, ADWEEK (Jan. 11, 2011), http://www.adweek.com/digital/social-media-is-free-social-media-marketing-is-not.

51. *See* Landcaster v. Alphabet Inc., No. 15-cv-05299-HSG, 2016 U.S. Dist. LEXIS 88908, at *6 (N.D. Cal. July 8, 2016).

52. *Id.*; Giveforward, Inc. v. Hodges, No. JFM-13-1891, 2015 U.S. Dist. LEXIS 102961, at *7 (D. Md. Aug. 6, 2015).

53. Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014).

54. *Section 230 of the Communication Decency Act*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230 (last visited Aug. 1, 2017).

55. Nathenson, *supra* note 21, at 110-11.

B. *The Rise of Social Media and New Terrorism*

The start of the new millennium marked the rise of social media.[56] In 2002, Friendster launched one of the first major social networking services to provide a vehicle for users to create their own personal communities online.[57] In 2003, more familiar platforms like LinkedIn and MySpace emerged.[58] Facebook, which has been referred to as the "king" that "resides upon the social networking throne," likely because of its 1.3 billion daily active users entered cyberspace in 2004,[59] followed by YouTube and Reddit just one year later.[60]

In the last decade, the influence of these social media companies has grown exponentially.[61] A Pew Research Center study showed that 90% of American young adults were active on social media in 2015, compared to the mere 12% in 2005.[62] That same study indicated that the modern trend to becoming more social media savvy extends beyond the nation's younger generations as two-thirds of the country's general population is now using social networking services, compared to the 7% of American users in 2005.[63] The United States is not the only country to experience the rise of social media, as it has become a global phenomenon.[64] As of May 2017, 2.51 billion people are reported active on social media and that number is projected to continually increase within the next few years.[65]

While there are many benefits resulting from the ability to better communicate on an international scale, the advent of social media has unfortunately contributed to a new age of terrorism that is much more extensive and dangerous than the terrorist plots seen in previous years.[66]

---

56. *See* Digital Trends Staff, *The History of Social Media*, DIGITAL TRENDS, http://www.digitaltrends.com/features/the-history-of-social-networking (last updated May 12, 2016).

57. *Id.*

58. Monica Riese, *The Definitive History of Social Media*, DAILY DOT, http://www.dailydot.com/debug/history-of-social-media (last updated Feb. 24, 2017).

59. Digital Trends Staff, *supra* note 56.

60. Riese, *supra* note 58.

61. *See* Andrew Perrin, *Social Media Usage: 2005–2015*, PEW RES. CTR. 2 (Oct. 8, 2015), http://www.pewInternet.org/2015/10/08/social-networking-usage-2005-2015.

62. *Id.* at 4.

63. *Id.*

64. *See* Dave Chaffey, *Global Social Media Research Summary 2017*, SMART INSIGHTS (Apr. 27, 2017), http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research.

65. *Id.*; *Number of Social Media Users Worldwide from 2010 to 2020 (in Billions)*, STATISTA, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users (last visited Aug. 1, 2017).

66. BRIAN MICHAEL JENKINS, *The New Age of Terrorism*, *in* THE MCGRAW-HILL HOMELAND SECURITY HANDBOOK 125-28 (2006).

Prior to social media's inception, past generations of terrorists relied on pamphlets, newsletters, and newspapers to spread their extremist message.[67] Following the attacks on September 11, 2001, terrorists moved to cyberspace to further disseminate their violent ideologies by creating their own websites.[68] However, this method became less desirable once Western intelligence and counterterrorist agencies began to uncover the terrorist-created sites.[69]

Due to its easy accessibility, inexpensive nature, and ability to "virtually 'knock on [users]' doors," social media has become the new method of communication for terrorists in the modern day.[70] It has been used as a "dark playground"[71] for terrorists, allowing them to communicate instantaneously with each other, provide training, fundraise, and recruit others to join the cause with the click of a button.[72] In contrast to "old terrorism" that was based on highly centralized, hierarchical networks, "new terrorism" is characterized by a cross-border cellular structure fostered by personal relationships that no longer require operational connections or face-to-face discussions.[73] One of the primary differences that distinguishes "new terrorism" from its outdated counterpart is that terrorists can now spread their message and news of successfully executed terrorist plots without having to rely on journalists to gain the public's attention.[74]

The interactive nature of social media has encouraged people who communicate on these platforms to see themselves as part of a broader jihadist movement, rather than mere spectators.[75] Terrorists recruited to join the jihadist movement often report a sense of brotherhood and inclusion in their endeavors, and attempt to lure other social media users seeking that same sense of belonging.[76] Terrorists' preferred methods to enlist potential sympathizers via social media include the posting of professionally created videos, live updates from the battlefield, and

67. JEROME P. BJELOPERA, CONG. RESEARCH SERV., R41416, AMERICAN JIHADIST TERRORISM: COMBATING A COMPLEX THREAT 20 (2013).

68. Weimann, *supra* note 11, at 2.

69. *Id.*

70. *Id.* at 3. For more information on how terrorists currently exploit the Internet, see Benjamin R. Davis, Comment, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet With the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119, 145-50 (2006).

71. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 10 (testimony of Mark Wallace, Chief Executive Officer, Counter Extremism Project).

72. BJELOPERA, *supra* note 67, at 22.

73. *Falkheimer*, *supra* note 30, at 146-47.

74. *Id.* at 148.

75. BJELOPERA, *supra* note 67, at 20-22.

76. *Id.* at 20.

personal dogmas encouraging others to carry out terror plots.[77] They often write eulogies for fallen members of the organization on social media, glamorizing terrorists who "sacrifice" themselves in the process of killing others as "martyrs" and depicting them as role models in the hopes that it will inspire others to follow suit.[78] Sometimes terrorists will use popular hashtags related to other trending news stories, such as "Ebola" or the "World Cup," in order to broadcast inciting material to a larger audience.[79] Much of the terrorist media dispersed online contains trademarks that authenticate the post, signaling to viewers that it came from the respective terrorist organization that produced it.[80]

In recent years, efforts to incite terror on social media have been rebranded to appeal to the Internet's younger audience.[81] This strategy may make terrorists' messages potentially more impactful as social media networks continue to be the most heavily utilized by users between the ages of eighteen to twenty-nine.[82] In fact, many American researchers warn that the increased radicalization of youth is not limited solely to the Middle East, but will also continue to become a significant issue at home.[83] The next Subpart discusses the recent

77. *See Falkheimer*, *supra* note 30, at 150-51 (examining ISIS's social media strategy implemented to radicalize users, classifying its approach into four levels).

78. Weimann, *supra* note 11, at 2.

79. Evan Perez et al., *Officials: U.S. Wants to Know how ISIS Recruited 3 Denver Teens*, CNN (Nov. 13, 2014), http://www.cnn.com/2014/11/12/us/isis-teen-recruitment.

80. *Jihadist Use of Social Media–How to Prevent Terrorism and Preserve Innovation: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H.R. Comm. on Homeland Sec.*, 112th Cong. 9 (2011) [hereinafter *Hearings on Jihadist Use of Social Media*] (statement of Andrew Aaron Weisburd, Director, Society for Internet Research).

81. Laura Huey, *This Is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming*, J. TERRORISM RES., May 2015, at 1-5. "Jihadi cool" is a recent phenomenon that has been popularized on social media, depicting Jihadist forms of terrorism into a "hip" subculture through the use of social media posts, videos, and other forms of propaganda aimed at the Internet's youth. *See id.* (discussing "jihadi cool," including depictions that have been shared on social media); *see also* Weimann, *supra* note 11, at 3 (discussing terrorists' "narrowcasting" strategy in which they specifically target younger users similar to how pedophiles lure their victims into online chatrooms).

82. Perrin, *supra* note 61. Terrorists' targeting of youth through the use of social media has been compared to the way gang members prey on at-risk teens in crime-ridden neighborhoods. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 13 (testimony of Mark Wallace, Chief Executive Officer, Counter Extremism Project).

83. *See, e.g.*, Margarita Bizina & David H. Gray, *Radicalization of Youth as a Growing Concern for Counter-Terrorism Policy*, GLOBAL SEC. STUD., Winter 2014, at 72-73 (evaluating the circumstances of the brothers responsible for the Boston bombing in 2013 to explain why younger people are becoming more active in terrorism); *see also* Marc Santora & Al Baker, *Arrests of 2 Men in Brooklyn Highlight New Challenges in Fighting ISIS*, N.Y. TIMES, Mar. 1, 2015, at A15 (discussing ISIS's creation of a video simulation based on the popular Grand Theft Auto game that was posted to Facebook and YouTube). In an effort to appeal to sympathizers in the West, ISIS members substituted the videogame's officers with those that look like New York City police officers to demonstrate how a militant could attack them. Santora & Baker, *supra*.

surge of homegrown terrorism in the United States and government attempts to address this issue that will continue to grow if it is not properly managed.[84]

C. *Homegrown Terrorism in the United States and the Federal Government's Response*

Social media and terrorism have rapidly risen, simultaneously, as terrorists continue to use social media networks to build their support and disperse information that sympathizers previously only had access to when joining foreign training camps.[85] The existence of terrorist propaganda on social media platforms has not only increased the number of terrorists affiliated with these organizations in the Middle East, but has subsequently resulted in the radicalization of many American citizens and spurred, as a result, a number of lone-wolf terrorist attacks in the United States.[86] It is for this reason that social media giants became the target of the Obama Administration and Congress.[87]

According to the Federal Bureau of Investigation ("FBI"), about 250 Americans have traveled to Syria and Iraq, or attempted to do so, to join the ranks of both ISIS and Al-Qaeda terrorist organizations in the year 2015.[88] A study conducted by the National Consortium for the Study of Terrorism and Responses to Terrorism ("START") found that only 37% of Americans attempting to travel to join terrorist organizations were influenced by the Internet in 2002 compared to the 83% in 2015, demonstrating that radicalization on the Internet has played an increasingly crucial role in inciting terror.[89] One of the most publicized recruitment attempts of an American citizen through the use of social media was the case of "Jihad Jane."[90] Known by her pseudonym "Jihad Jane," forty-six-year-old Colleen LaRose of Pennsylvania became radicalized online and outwardly expressed her dedication to the jihadist cause through the use of YouTube, Twitter, and MySpace.[91] Plotting with another terrorist over the Internet, she and her

84. *See infra* Part II.C.

85. BJELOPERA, *supra* note 67, at 23.

86. *See* Chris Strohm, *Lone-Wolf Terrorism*, BLOOMBERG (May 23, 2017), https://www.bloomberg.com/quicktake/lone-wolf-terrorism (last updated May 23, 2017).

87. *Digital Developments: Extremists' Use of Modern Communication Tools*, COUNTER EXTREMISM PROJECT, http://www.counterextremism.com/content/digital-developments-extremists-use-modern-communication-tools (last visited Aug. 1, 2017).

88. S. REP. NO. 114-295, at 2 (2016).

89. *Id.* at 3.

90. Weimann, *supra* note 11, at 11.

91. David Sapsted, *'Jihad Jane' Was Tracked by Amateur Internet Sleuths*, NATIONAL (Mar. 17, 2010), http://www.thenational.ae/news/world/americas/jihad-jane-was-tracked-by-amateur-

co-conspirator agreed to marry and travel to Sweden, coordinating an attempt to murder a Swedish cartoonist as a form of revenge for his controversial depiction of the Prophet Mohammed that angered many Muslims worldwide.[92] She was known to have actively solicited funding for Al-Qaeda and its supporters until she was arrested upon her return from Europe.[93] While "Jihad Jane" was one of the first known cases of an American citizen inspired to commit acts of terror based on inciting material she had seen on social media, she certainly was not the last.[94]

The FBI also submitted a report before the Senate Committee on Homeland Security and Governmental Affairs showing that instances of homegrown terrorist attacks have more than doubled since 2009.[95] Some of the most notable attacks in recent years, including, but not limited to the Boston Marathon bombing,[96] and the shootings in Garland, Texas,[97] San Bernardino, California,[98] and Pulse Nightclub in Orlando, Florida,[99]

Internet-sleuths. She consistently pledged her allegiance to "Sheikh OBL [Osama Bin Laden] and brothers in jihad" and proclaimed her aim to die as a martyr for the jihadist cause. *Id.*

92. *Id.* The provocative cartoon that enraged the Muslim community in 2007 was created by Swedish national Lars Vilks and depicted the Prophet Mohammed as a dog. Paula Newton, *Artist Defiantly Draws Prophet Mohammed*, CNN (Oct. 16, 2007), http://www.cnn.com/2007/WORLD/europe/10/16/artist.controversy/. To view the cartoon, see Lauren Barbato, *Why Controversial Cartoonist Lars Vilks Has Become a Target of Islamic Terrorists*, BUSTLE (Feb. 14, 2015), https://www.bustle.com/articles/64366-why-controversial-cartoonist-lars-vilks-has-become-a-target-of-islamic-terrorists.

93. *See* BJELOPERA, *supra* note 67, at 87-88.

94. *See, e.g.*, Joshua Berlinger & Catherine E. Schoichet, *Mississippi Woman Pleads Guilty on Charge That She Tried to Join ISIS*, CNN (Mar. 30, 2016), http://edition.cnn.com/2016/03/30/us/mississippi-isis-guilty-plea-jaelyn-young (discussing the plan of a young, newly engaged couple from Mississippi using their wedding and honeymoon as a cover to travel to Syria and join ISIS in 2015); Ben Brumfield, *Officials: 3 Denver Girls Played Hooky from School and Tried to Join ISIS*, CNN (Oct. 22, 2014, 10:28 AM), http://www.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey (noting that three teenage girls from Denver skipped school to join ISIS members in Syria in 2014); Helen Coster, *The Long Island Jihadist*, NEW YORKER (Nov. 26, 2013), http://www.newyorker.com/news/news-desk/the-long-island-jihadist (following a Long Island, New York teen attempting to flee to Yemen to join the Ansar al-Sharia terrorist group in 2013).

95. S. REP. NO. 114-295, at 2 (2016).

96. Michael Cooper, et al., *Boston Suspects Seen as Zealots and Self-Taught*, N.Y. TIMES, Apr. 24, 2013, at A1 (reporting that the Boston bombers were not acting with a known terrorist group but instead were self-radicalized from inciting materials found on the Internet).

97. Ed Payne, *Texas Shooting: Despite ISIS Claims, Did Terror Group Play a Role?*, CNN (May 6, 2015), http://www.cnn.com/2015/05/06/us/garland-texas-prophet-mohammed-contest-shooting (noting that the gunman was communicating with ISIS members via Twitter regardless of whether he was directed by ISIS leaders to carry out the attack or did it on his own volition as a lone-wolf).

98. Pamela Engel, *San Bernardino Shooter Allegedly Pledged Allegiance to ISIS' Leader on Facebook*, BUS. INSIDER (Dec. 4, 2015, 10:50 AM), http://www.businessinsider.com/san-bernardino-shooter-isis-cnn-2015-12 (reporting that the female shooter pledged her allegiance to ISIS on Facebook in the midst of the attack). ISIS has been known to instruct sympathizers on Twitter to declare their allegiance to the group prior to carrying out an attack. *Id.*

99. Mark Follman, *The Orlando Mass Shooter Checked Facebook for News of His Attack as*

have been connected to some form of online radicalization whether it be self-taught through inciting material already present on social media or due to communications with actual terrorist groups via social media platforms.[100] ISIS-inspired terror attacks have also become increasingly more prevalent on college campuses,[101] as evidenced by the stabbing attacks at UC Merced[102] and Ohio State.[103] Many experts believe that the rise of homegrown, lone-wolf terrorist attacks in the United States is the result of terrorists' message to sympathizers urging that "if you cannot travel, kill where you are."[104]

As homegrown terrorism becomes an increasingly more serious issue, the White House has attempted to pressure social media companies into better controlling terrorists' abuse of their services in recent years.[105] In December 2015, former Secretary of State Hillary Clinton spoke before a forum held by the Brookings Institution, calling for a more aggressive response from social media companies to restrict terrorist presence on their platforms.[106] She stated that companies should aim to "[r]esolve means depriving jihadists of virtual territory, just as [the federal government] work[s] to deprive them of actual territory," to ensure the safety of the American people.[107] After finding that it was

---

He Killed, MOTHER JONES (June 17, 2016, 4:37 PM), http://www.motherjones.com/politics/2016/06/orlando-mass-shooter-social-media-copycat-motive (explaining that the shooter was not only inspired to commit the attack because of inciting material found on social media, but actually was checking Facebook to see reports of his attack while holding victims hostage).

100. *See supra* notes 96-99 and accompanying text.

101. *See, e.g.*, Devlin Barrett, *Boston Police Captain's Son Arrested in ISIS-Inspired Plot*, WALL ST. J. (July 13, 2015, 4:15 PM), http://www.wsj.com/articles/boston-police-captains-son-arrested-in-isis-inspired-plot-1436816697 (discussing the arrest of a twenty-three-year-old man who was plotting a terror attack aimed at students in the cafeteria and dorms of an unidentified college campus in Massachusetts).

102. Melissa Chan, *UC Merced Stabber Faisal Mohammad Was Carrying ISIS Flag; Teen's Family Offers Sympathy for Victims, Says Son was 'Kind and Respectful'*, N.Y. DAILY NEWS (Nov. 11, 2015, 10:48 AM), http://www.nydailynews.com/news/national/uc-merced-stabber-faisal-mohammad-carrying-isis-flag-article-1.2430980. An ISIS flag was discovered in the backpack of a California freshman at UC Merced after he stabbed four of his classmates in November 2015. *Id.*

103. Sarah Volpenhein, et al., *Ohio State Attacker Described Himself as a 'Scared' Muslim*, DAILY BEAST (Nov. 28, 2016, 3:54 PM), http://www.thedailybeast.com/articles/2016/11/28/attack-with-butcher-knife-and-car-injures-several-at-ohio-state-university.html. In November 2016, an Ohio State student intentionally struck his classmates with his car and proceeded to stab them. *Id.* While there is no evidence that the attacker had any direct ties to ISIS, the attack occurred only two days after ISIS leaders called for its sympathizers in the West to carry out attacks with weapons that would go unnoticed by authorities, such as knives and homemade explosives. *Id.*

104. S. REP. NO. 114-295, at 2 (2016).

105. *See* COUNTER EXTREMISM PROJECT, *supra* note 87.

106. David E. Sanger, *Clinton Urges Silicon Valley to 'Disrupt' Islamic State Through its Internet Access*, N.Y. TIMES, Dec. 7, 2015, at A16.

107. Nicole Perlroth & Mike Isaac, *Terrorists Mock Bids to End Use of Social Media*, N.Y. TIMES, Dec. 8, 2015, at A1.

"technically feasible" for tech companies to provide law enforcement agencies with the ability to access encrypted, coded messages on social media platforms, the Obama Administration urged social media companies to devise their own decryption abilities specific to their unique systems.[108] Former President Obama also encouraged these companies to assist law enforcement in acquiring intelligence information, but this became a highly contested issue that was not well received by social media giants, tech companies, or individuals concerned with the need for privacy rights free from government intrusion.[109]

While the battle to fight terrorism has remained an international effort,[110] members of Congress have continually demanded a more forceful national approach to reduce the number of Americans enlisted to commit terrorism and curb the growth of homegrown terrorism in the United States;[111] their proposed solution begins with restricting terrorists' use of social media.[112] Since the leading social media platforms, namely Facebook, Twitter, and YouTube, are American corporations subject to U.S. law, these companies have become the focus of legislators, as they also tend to be the most heavily utilized by terrorists.[113]

Although Congress has not yet received bicameral support for an act regarding terrorists' use of social media specifically, legislation seeking to address terrorism in the U.S. does exist.[114] The Uniting and

---

108. *See* COUNTER EXTREMISM PROJECT, *supra* note 87.

109. *Id.* The debate over whether the government can legally compel companies to provide encrypted messages for intelligence purposes raises Fourth Amendment privacy concerns for those in opposition to increased government surveillance. *See, e.g.*, Keir Lamont, *The Human Rights Problem with Social Media Monitoring*, ACCESSNOW (Jan. 8, 2016, 10:55 AM), https://www.accessnow.org/13503-2. Since this Note is limited to terrorist incitement on social media that is intended for public viewing, Fourth Amendment issues are beyond the scope of this Note. For a brief discussion on the relationship between social media and the Fourth Amendment, see Alexandra Paslawsky, Note, *The Growth of Social Media Norms and Governments' Attempts at Regulation*, 35 FORDHAM INT'L L.J. 1485, 1497-1500 (2012).

110. Barak-Erez & Scharia, *supra* note 47, at 19-23; Davis, *supra* note 70, at 151-62.

111. *See Hearings on Jihadist Use of Social Media*, *supra* note 80, at 2 (statement of Patrick Meehan, Chairman of Subcomm. on Counterterrorism & Intelligence) ("[W]e cannot ignore the reality that we have been unable to effectively prevent jihadi videos and messages from being spread on popular social media websites like YouTube and Facebook.").

112. *See* S. REP. NO. 114-295, at 5 (2016). Congress has called for legislation that would require the President to deliver to Congress a report on the U.S. government's strategy to combat terrorist organizations' use of social media. *See, e.g.*, *id.* (suggesting the Combat Terrorist Use of Social Media Act of 2016); H.R. 3654, 114th Cong. (2015) (displaying the House of Representative version of the Combat Terrorist Use of Social Media Act of 2015).

113. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 10 (testimony of Mark Wallace, Chief Executive Officer, Counter Extremism Project).

114. *See* S. 2517, No. 114-295.

Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"),[115] was passed almost unanimously in response to the September 11, 2001, attack on the World Trade Center.[116] Aside from often being accused of going too far in expanding the government's ability to surveil its citizens,[117] the PATRIOT Act has been criticized for focusing too narrowly on deterrence measures, such as its imposition of harsher sentences on those found engaging in cyber terrorist attacks, on the grounds that these provisions are more reactionary, rather than preventative, in nature.[118] Although this result was likely incidental, plaintiffs have recently cited portions of the PATRIOT Act in cases that assess social media's role in managing terrorist incitement on their platforms, often referencing the PATRIOT Act's "Material Support" statute ("Material Support Statute"), currently codified in 18 U.S.C. §§ 2339A–2339B.[119] As these plaintiffs continue to base their theory of liability on the Material Support Statute, its relevance and application could increase in the future.[120]

---

115. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C., 22 U.S.C., 28 U.S.C., 47 U.S.C., and 50 U.S.C.).

116. *The USA PATRIOT Act: Preserving Life and Liberty*, DEP'T JUST., https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (last visited Aug. 1, 2017).

117. *See* Sue Udry, *Happy Birthday Patriot Act! For Fifteen Years You Have Done Your Best to Crush Democracy. But You Haven't Won Yet.*, DEFENDING RTS. & DISSENT (Oct. 26, 2016), http://bordc.org/news/happy-birthday-patriot-act-fifteen-years-done-best-crush-democracy. The passing of the PATRIOT Act still remains a controversial issue. The Bill of Rights Defense Committee recently claimed the law "ripped the Fourth Amendment to shreds." *Id.* Similar to its position on the original provisions of the CDA, the ACLU has also staunchly opposed the PATRIOT Act for violating Americans' civil liberties. *See Surveillance Under the PATRIOT Act*, ACLU, https://www.aclu.org/infographic/surveillance-under-patriot-act (last visited Aug. 1, 2017).

118. Davis, *supra* note 70, at 151-53.

119. *See infra* Part III.A. The Material Support Statute makes it a crime to provide "material support" to any designated foreign terrorist organization. 18 U.S.C. § 2339A (2012). The term "material support" is defined as the following:

> [A]ny property, tangible or intangible, or service, including currency or monetary instruments or financial securities, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

18 U.S.C. § 2339A(b)(1). The Material Support Statute derives from previous acts created to address terrorism in the past. For a brief discussion on the PATRIOT Act's expansion of the Material Support Statute, see Todd M. Gardella, Note, *Beyond Terrorism: The Potential Chilling Effect on the Internet of Broad Law Enforcement Legislation*, 80 ST. JOHN'S L. REV. 655, 657-61 (2006).

120. *See infra* Part III.A. *But see* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009) ("[T]he language of [section 230] does not limit its application to defamation cases.").

III. SECTION 230'S AUTOMATIC PROTECTION OF INTERNET SERVICE PROVIDERS FAILS TO INCENTIVIZE ACTION

Section 230's safe harbor provision of the CDA has consistently provided automatic immunity to ISPs for content posted by third parties, which has led courts to rarely consider claims against social media platforms beyond the pleading stage.[121] Subpart A discusses how courts have recently treated claims against ISPs that have been accused of providing "material support" to terrorists by their adversaries.[122] Subpart B explains how ISPs' lack of legal obligation to take down inciting material has resulted in a failure to cooperate on the part of social media companies that staunchly support freedom of expression, while it has led to inconsistent, and sometimes inadequate, approaches by those companies that do attempt to manage terrorists' use of their services.[123] Subpart C highlights the obstacles presented by the First Amendment when trying to address this issue, demonstrating that the United States must create a more unique approach compared to its global counterparts who are able to create content-based limitations on speech.[124]

A. Cases Against Internet Service Providers Are Dismissed Almost Immediately in Terrorist Context

Due to section 230's automatic insulation from liability, many of the recent cases filed by victims of terror and their families against social media giants tend to be dismissed at the very early stages of litigation.[125] The plaintiffs in these types of cases, such as *Fields v. Twitter*,[126] *Gonzalez v. Twitter*,[127] and *Force v. Facebook*,[128] base their theories of liability on the Material Support Statute provisions, 18 U.S.C. §§ 2339A–2339B, which forbid any person or institution from providing

121. *See, e.g.*, Klayman v. Zuckerberg, 910 F. Supp. 2d 314, 321 (D.D.C. 2012) (granting defendant's motion to dismiss due to section 230's grant of automatic immunity in a case involving a Facebook page advocating for the Third Palestinian Intifada).

122. *See infra* Part III.A.

123. *See infra* Part III.B.

124. *See infra* Part III.C.

125. *See, e.g.*, Russell Brandom, *Twitter Is Not Legally Responsible for the Rise of ISIS, Rules California District Court*, VERGE (Aug. 10, 2016, 4:00 PM), http://www.theverge.com/2016/8/10/11950098/twitter-isis-lawsuit-safe-harbor-terrorism.

126. Complaint at 14-15, Fields v. Twitter, Inc., 2016 LEXIS 161233, at *28-32 (N.D. Cal. Nov. 18, 2016) (No. 16-cv-00213-WHO).

127. Verified Complaint at 31-32, Gonzalez v. Twitter, Inc., No. 3:16-cv-03282 (N.D. Cal. June 14, 2016).

128. Amended Complaint at 2-3, Force v. Facebook, Inc., No. 1:16-cv-05158-NGG-LB (E.D.N.Y. July 10, 2016).

"material support" to recognized foreign terrorist organizations.[129] Lawyers and legal scholars predict, however, that these types of cases are not going to gain much momentum due to section 230's precedential reign.[130]

Fields is a case that was filed by the wife of Lloyd Fields, an American contractor who was killed in an ISIS-driven shooting attack in Amman, Jordan on November 9, 2015.[131] Plaintiff Tamara Fields claims that Twitter "knowingly permitted the terrorist group ISIS to use its social media network as a tool for spreading extremist propaganda, raising funds, and attracting new recruits," constituting "material support."[132] The complaint provides a number of images that were once posted on Twitter by pro-ISIS accounts promoting terrorism, including an image combining the Twitter logo with the ISIS flag.[133] The complaint alleges that ISIS members claimed responsibility and boasted of the attack, stating that it will continue to influence other sympathizers who will eventually transform into lone wolves through the use of Twitter's services.[134] Plaintiffs unsuccessfully argued that because they did not seek to hold Twitter accountable as "publisher" of the inciting material posted by terrorists, Twitter should not be entitled to automatic protection under section 230.[135] The case against Twitter was quickly

---

129. 18 U.S.C. §§ 2339A–2339B (2012); *see supra* notes 126-128.

130. *See, e.g.*, Cyrus Farivar, *It'll be Very Hard for Terrorism Victim's Family to Win Lawsuit Against Twitter*, ARS TECHNICA (June 17, 2016, 5:00 AM), http://arstechnica.com/tech-policy/2016/06/itll-be-very-hard-for-terrorism-victims-family-to-win-lawsuit-against-twitter; Kevin Walsh et al., *New Suits Against Social Media Giants Seek to Expand Reach of U.S. Anti-Terrorism Laws*, INSIDE COUNSEL (Aug. 9, 2016), http://www.insidecounsel.com/2016/08/09/new-suits-against-social-media-giants-seek-to-expa?slreturn=1477867434 (referring to these types of cases as "improbable"). *But see* Zoe Bedell & Benjamin Wittes, *Tweeting Terrorists, Part I: Don't Look Now but a Lot of Terrorist Groups Are Using Twitter*, LAWFARE (Feb. 14, 2016, 5:05 PM), https://www.lawfareblog.com/tweeting-terrorists-part-i-dont-look-now-lot-terrorist-groups-are-using-twitter (arguing that Twitter "probably" is openly violating the Material Support Statute); Benjamin Wittes & Zoe Bedell, *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 (analyzing the strengths of plaintiffs' argument in *Force*).

131. Complaint, *supra* note 126, at 1.

132. *Id.* at 1, 14.

133. *Id.* at 1-2.

134. *Id.* at 13-14.

135. Fields v. Twitter, Inc., No. 16-cv-00213-WHO, 2016 LEXIS 161233, at *28-32 (N.D. Cal. Nov. 18, 2016). Instead, plaintiffs were seeking to hold Twitter accountable for providing material support to ISIS in violation of the Material Support Statute. Fields v. Twitter, No. 16-cv-00213-WHO, 2016 LEXIS 105768, at *11 (N.D. Cal. Aug. 10, 2016) ("[Twitter's] violations of the [Material Support Statute] cannot be accurately characterized as publishing activity, but rather as the provision of the means through which ISIS spreads its poison."). This is the second time the case was dismissed. *Id.* Judge William Orrick had already previously dismissed the case with leave to amend back in August 2016. *Id.*

dismissed because, according to Judge Orrick, "[a]part from the private nature of Direct Messaging, plaintiffs identify no way in which their Direct Messaging theory seeks to treat Twitter as anything other than a publisher of information provided by another content provider."[136]

Family members of Nohemi Gonzalez, a twenty-three year-old who was the sole American victim of the 130 people killed in the ISIS-driven terror attacks in Paris on November 13, 2015, recently sued Google (in its capacity as owner of YouTube), Facebook, and Twitter for reasons analogous to those stated by the plaintiffs in *Fields*.[137] Similarly filed in the U.S. District Court of Northern California, the plaintiffs in *Gonzalez* claim that the companies "knowingly permitted the terrorist group ISIS to use their social networks as a tool for spreading extremist propaganda, raising funds, and attracting new recruits" in violation of the Material Support Statute.[138] The complaint alleged that "[t]hrough Defendants' sites, ISIS disseminates its official media publications as well as posts about real-time atrocities and threats to its perceived enemies" and then listed a number of examples of these aforementioned atrocities, including a tweet posted by an Australian ISIS member that displayed a photo of his seven-year-old son holding the decapitated head of a Syrian soldier.[139]

Force is only slightly different from the other recent attempts by victims of terror to hold social media companies accountable for allowing terrorist activity to remain on their platforms in that it was filed in the U.S. District Court for the Eastern District New York and focuses on the social media presence of the Palestinian terrorist group Hamas, rather than ISIS.[140] But legal experts say that this case may be a breakthrough in the line of Material Support cases and could potentially survive a motion to dismiss.[141] The plaintiffs in this case include the

136. *Fields*, 2016 LEXIS 161233 at *32. In ordering the dismissal, Judge Orrick focused on plaintiffs' Direct Messaging theory, rather than the ISIS posts that were made for public viewing, likely because plaintiffs contended that their claims were not based on "the content of the tweets, the issuing of the tweets, or failure to remove the tweets" in trying to avoid the CDA's application. *Id.* at *11.

137. Dan Bilefsky, *American Was Pursing Her Dreams of Design in Paris*, N.Y. TIMES, Nov. 20, 2015, at A16; Jacob Bogage, *Family of ISIS Paris Attack Victim Sues Google, Facebook and Twitter*, WASH. POST (June 16, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/06/16/family-of-isis-paris-attack-victim-sues-google-facebook-and-twitter. Although the plaintiffs in the two cases are represented by different legal counsel, many of the same images used in the *Fields* complaint were featured in that of *Gonzalez Paris Victim's Father Sues Twitter, Facebook, Google Over ISIS*, CBS NEWS (June 15, 2016, 9:50 PM), http://www.cbsnews.com/news/paris-attacks-victim-sues-twitter-facebook-google-youtube-isis-nohemi-gonzalez.

138. Verified Complaint, *supra* note 127, at 2.

139. *Id.* at 12-13.

140. *See* Amended Complaint, *supra* note 128, at 1-2.

141. Wittes & Bedell, *supra* note 130. For a discussion on why the *Force* complaint may

families of victims from five separate terror attacks that took place in Israel between the years 2014 and 2016.[142] They claim that Facebook "knowingly provided material support and resources to Hamas" and therefore, "violated the federal prohibitions on providing material support or resources for acts of international terrorism."[143] The complaint provides many examples of Hamas' open and extensive presence on Facebook and attempts to demonstrate the direct causation between terrorist use of the platform and its connection with the specific attacks related to the victims whose families are suing on their behalf.[144] While the suit remains in its early stages, Facebook representatives met with Israeli government officials soon after the case was filed, acknowledging that more needs to be done to eliminate terrorist incitement on its platform.[145]

While it seems as though the success of these plaintiffs' claims is unlikely due to ISPs' lack of legal obligation, courts appear to have started to question section 230's automatic immunity in the context of defamation claims and privacy issues.[146] Recently, judges seem to be more willing to hold these social media companies accountable for the content on their platforms in situations when the platforms were notified of the defamatory content and failed to comply with a user's takedown request after promising to do so.[147] Some scholars believe that Congress

---

provide a stronger showing of causation between the terrorist organization's social media presence and the resulting terror attacks, which was deemed a major flaw in the *Fields* and *Gonzalez* cases, see *id.*

142. Amended Complaint, *supra* note 128, at 2. There were six victims: Yaakov Naftali Fraenkel, a sixteen-year-old who was one of three teens abducted and murdered by HAMAS members in 2014; Chaya Zissel Braun, a three-month-old baby who was fatally injured when a HAMAS terrorist intentionally drove his car into a Jerusalem light rail train station in 2014; Richard Lakin, a seventy-six-year-old who was shot and stabbed to death by a terrorist while riding a public bus in 2015; Taylor Force, a twenty-nine-year-old American M.B.A. student on a school-sponsored trip who was stabbed to death while walking the Jaffa boardwalk in 2016; and Menachem Mendel Rivkin, who was stabbed by a terrorist on his way to a restaurant in 2016, but eventually overcame his injuries. *See id.* at 29-100.

143. *Id.* at 2-3.

144. Wittes & Bedell, *supra* note 130.

145. Gwen Ackerman, *Facebook and Israel Agree to Tackle Terrorist Media Together*, BLOOMBERG (Sept. 12, 2016, 2:18 PM), http://www.bloomberg.com/news/articles/2016-09-12/facebook-and-israel-agree-to-tackle-terrorist-media-together.

146. Reuters, *Judges Are No Longer Giving Tech Companies an Automatic Pass on Civil Liability*, FORTUNE (Aug. 18, 2016, 5:02 PM), http://fortune.com/2016/08/18/judges-tech-companies.

147. *See, e.g.*, Edward Fenno & Christina Humphries, *Protection Under CDA §230 and Responsibility for "Development" of Third-Party Content*, 28 A.B.A. COMM. LAWYER, Aug. 2011, at 1, 28-29; Eric Goldman, *Craigslist Loses 230 Defense to Promissory Estoppel Claim–Scott P. v. Craigslist*, TECH. & MARKETING L. BLOG (June 11, 2010), http://blog.ericgoldman.org/archives/2010/06/craigslist_lose.htm.

never intended to provide automatic insulation from liability in the first place.[148] This recent trend has not yet extended to cases in which plaintiffs sue social media companies for failing to adequately manage the terrorist incitement on their platforms, but could demonstrate a willingness to possibly do so in the future.[149]

B. Lack of Legal Obligation for Internet Service Providers Leads to Inconsistent Cooperation and Approaches

While many believe that social media giants have a moral responsibility to hinder terrorists' ability to incite violence publicly on their services, it is almost universally accepted that there is currently no legal obligation to do so in the United States.[150] Those who urge these companies to remove terrorist incitement on their platforms often complain of the lack of cooperation they encounter when making these requests.[151] For example, Mark Wallace, CEO of the Counter Extremism Project ("CEP"), recounted before the Senate Subcommittee on Terrorism, Nonproliferation, and Trade his experience contacting Twitter on three separate occasions before receiving a seemingly lackluster response from Twitter personnel, characterizing Twitter's efforts to remedy this problem as almost negligent.[152]

A quote from the CEO of CloudFlare—an online chat forum whose employees were recently accused of protecting terrorists' ability to use the site—depicts the sentiment of many media giants that refuse to comply with users' takedown requests of terrorist incitement.[153] He stated, "A Web site is speech. It is not a bomb. There is no imminent danger it creates and no provider has an affirmative obligation to monitor and make determinations about the theoretically harmful nature of speech a site may contain."[154] It is important to note that Twitter has since taken a much more aggressive approach in managing this issue by

148. Ehrlich, *supra* note 35, at 408-11.

149. *See, e.g.*, Fields v. Twitter, Inc., No. 16-cv-00213-WHO, 2016 LEXIS 161233, at *2 (N.D. Cal. Nov. 18, 2016) ("As horrific as these deaths were, under the CDA Twitter cannot be treated as a publisher or speaker of ISIS's hateful rhetoric and is not liable under the facts alleged.").

150. *See, e.g.*, Patricia Hurtado, *Facebook and Its Lawyers Slammed by Judge in Terrorism Suits*, BLOOMBERG (Sept. 22, 2016, 8:27 PM), http://www.bloomberg.com/news/articles/2016-09-22/facebook-and-its-law-firm-slammed-by-judge-in-terrorism-suits (quoting a seemingly frustrated judge presiding over a suit against Facebook who asked, "Doesn't Facebook have some moral obligation to help cabin the kinds of communications that appear on it?").

151. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 11-12 (testimony of Mark Wallace, Chief Executive Officer, Counter Extremism Project).

152. *Id.* at 11.

153. *Id.* at 47 (statement of Evan Kohlmann, Chief Information Officer, Flashpoint Partners).

154. *Id.*

suspending 235,000 accounts in a span of six months, but skeptics are quick to characterize their efforts as a brief period of cooperation that will likely subside once the company is no longer forced to take action "to save public face."[155]

Most social media companies currently do attempt to accommodate law enforcement and users in their demands for more aggressive management of terrorist incitement on their services.[156] Many social media intermediaries try to do so by removing offensive language that violates the platforms' terms of service, blocking access to sites, or terminating user profiles.[157] Facebook's, YouTube's, and Twitter's "Terms of Service" all explicitly state that calls for violence and terrorism will not be permitted on the platform.[158] Facebook has been revered as one of the more cooperative social media companies in that it has proactively sought to limit the amount of inciting content present on its platform prior to receiving takedown requests.[159] However, reports show that Facebook was not always as willing to remove terrorist incitement on its platform as it is today.[160] In the past, YouTube has been accused of placing advertisements before the start of ISIS videos.[161]

155. *Id.* (claiming that Twitter only reacted to takedown requests when the video of James Foley's beheading surfaced on the platform to maintain a reputable image in the public eye); Katie Benner, *Twitter Adds to the List of Supsended Accounts*, N.Y. TIMES, Aug. 19, 2016, at B2.

156. *See, e.g.*, *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 2 (commending Facebook and YouTube for increasing their efforts to proactively remove terrorist incitement on their platforms).

157. Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1468-71 (2011).

158. *Community Standards*, *supra* note 17 ("We don't allow for any organizations that are engaged in [terrorist activity] to have a presence on Facebook."); *The Twitter Rules*, *supra* note 17 ("You may not make threats of violence or promote violence, including threatening or promoting terrorism."); *YouTube Community Guidelines*, *supra* note 17 ("YouTube strictly prohibits content intended to recruit for terrorist organizations, incite violence, celebrate terrorist attacks or otherwise promote acts of terrorism.").

159. Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015, 7:00 AM), https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media.

160. *See, e.g.*, Rahat Husain, *Husain: Facebook Refuses to Take Down ISIS Terror Group Fan Page*, WASH. TIMES (June, 16, 2014), http://www.washingtontimes.com/news/2014/jun/16/husain-facebook-refuses-take-down-isis-terror-grou (discussing a known ISIS-affiliated fan page that Facebook initially refused to take down because the content did not constitute "hate speech" according to its "Community Standards" guidelines). The page was subsequently removed an hour after this article was posted. *Id.* The plaintiff in *Force* made a similar grievance, alleging that when Facebook was notified of the incendiary content, it would reply by saying the post did not violate its policies or would delete a portion of the content, but still allow the page to remain on the platform. Amended Complaint, *supra* note 128, at 109.

161. Laurie Segall, *These Ads Ran Before ISIS Videos*, CNNMONEY (Mar. 3, 2015, 7:09 PM), http://money.cnn.com/2015/03/03/technology/isis-ads-youtube (reporting that YouTube placed ads for Aveeno skin products, Budweiser beer, and Secret deodorant before extremist ISIS videos). Companies purchasing advertisements on YouTube do not control which videos their ads will be

Both Facebook and YouTube have since instituted reporting mechanisms that allow its users to flag incendiary content that promotes terrorist activity.[162] Additionally, Facebook, Microsoft, Twitter, and YouTube recently announced that they will be joining forces in their efforts to combat terrorists' use of their services through the creation of a shared database that will form "digital fingerprints" of terrorist images so that other participating companies can more easily identify the same content on their own platforms.[163] But even so, these efforts are voluntary,[164] are often not transparent,[165] and do not always meet the expectations of the general public.[166]

C. *First Amendment Freedom of Speech Protection Does Not Allow for Content-Based Limitations on Speech*

The spread of terrorism to social media is an international issue that many civilized nations seek to address.[167] Countries like France, Israel,

---

used in conjunction with, and many of these companies were upset with the platform for having their products associated with videos posted by the terrorist organization. *Id.*

162. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 42 (statement of J.M. Berger, Nonresident Fellow, the Brookings Institution).

163. Associated Press, *Facebook, Microsoft, Twitter & YouTube Team Up to Fight Terrorist Propaganda*, L.A. TIMES (Dec. 5, 2016, 4:20 PM), http://www.latimes.com/business/technology/la-fi-tn-Internet-terrorism-20161205-story.html. This joint effort was initiated in response to pending federal legislation that would require social media companies to notify law enforcement any time they became aware of online terrorist activity. *Id.* The four companies spearheading the campaign against terrorist activity on social media plan on expanding access to the database to other companies in the future. *Id.*

164. Bambauer, *supra* note 17, at 88.

165. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 44 (statement of J.M. Berger) ("All stakeholders need to clearly understand exactly why and how a user gets suspended on social media. Companies need to communicate this better.").

166. *See* Hurtado, *supra* note 150 (discussing a Brooklyn judge's accusation that Facebook was not taking suits involving risks of international terrorism seriously after the company's legal team sent a first-year associate to a hearing); Naina Khedekar, *Anti-Terrorism Policies: How Facebook and Twitter Tackle Terrorism Online*, TECH2 (July 15, 2016, 4:54 PM), http://tech.firstpost.com/news-analysis/how-facebook-and-twitter-tackle-terrorism-online-325292.html. (referencing a Change.org petition signed by over 140,000 users following the Paris attacks demanding that Facebook respond more quickly to content removal requests); *Demand Action From Social Media Companies*, COUNTER EXTREMISM PROJECT, http://www.counterextremism.com/content/petition-1 (last visited Aug. 1, 2017) (urging users to sign a petition demanding further action from social media companies to curb ISIS members' use of their services).

167. *See* U.N. OFFICE ON DRUGS & CRIME, THE USE OF THE INTERNET FOR TERRORIST PURPOSES (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf ("The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner." (quoting Ban Ki-moon, Sec'y-Gen. of the United Nations)). While the United Nations' Security Council has adopted many resolutions devoted to counter terrorism, the United Nations primarily urges its member states to address the issue of terrorism on the Internet through domestic legislation because it can be more tailored to each individual government's circumstances. *Id.* at 16-17, 23-24.

Spain, and the United Kingdom that are similarly determined to restrict the use of social media for terrorist purposes have tried to resolve the issue by creating content-based limitations on speech, sometimes employing balancing tests to determine whether the speech in question is worthy of protection.[168] However, due to the reverence of the First Amendment in the United States, the methods by which the federal government can check terrorist incitement on social media is more limited compared to its international counterparts.[169]

The First Amendment guarantees the freedoms of speech and association to the American public by mandating that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people to peaceably assemble."[170] This has historically been interpreted to mean that the federal government cannot limit citizens' ability to express themselves based on the idea or message communicated through their expression.[171] The right to speak freely is one of the most fervently protected rights for civil liberties advocates seeking to ensure that Americans may enjoy the individual liberties provided for in the Constitution.[172] While the right to freedom of speech has always been heavily guarded, it was never absolute.[173] Historically, free speech rights tend to be most tested during times of war or unrest, usually in matters related to national security.[174]

The Supreme Court's view became much clearer through its discussion involving speech advocating violence in the landmark

168. *See* Barak-Erez & Scharia, *supra* note 47, at 5-14; *see, e.g.*, Haviv Rettig Gur & Stuart Winer, *Bill Cracking Down on Social Media Incitement Passes Initial Reading*, TIMES ISRAEL (July 20, 2016, 6:19 PM), http://www.timesofisrael.com/bill-cracking-down-on-social-media-incitement-passes-initial-reading.

169. *See* Barak-Erez & Scharia, *supra* note 47, at 14-19.

170. U.S. CONST. amend. I.

171. Paslawsky, *supra* note 109, at 1495.

172. *See, e.g.*, *Free Speech*, ACLU, https://www.aclu.org/issues/free-speech (last visited Aug. 1, 2017).

173. ANTHONY LEWIS, FREEDOM FOR THE THOUGHT THAT WE HATE: A BIOGRAPHY OF THE FIRST AMENDMENT 12-13 (2007).

174. Abigail M. Pierce, Note, *#Tweeting for Terrorism: First Amendment Implications in Using Proterrorist Tweets to Convict under the Material Support Statute*, 24 WM. & MARY BILL RIGHTS J. 251, 257-59 (2015). The same men that adopted the First Amendment were responsible for passing the Sedition Act seven years later, which criminalized the publication of "false, scandalous, and malicious writing against the [g]overnment" when its intent was to defame or stir an uprising. *Id.* at 256. The Sedition Act was passed in response to the French Revolution because government officials feared that French Terrorism would spread to the United States. LEWIS, *supra* note 173, at 12; *see also* Schenk v. United States, 249 U.S. 47, 52 (1919) (denying First Amendment protections to a defendant convicted under the Espionage Act for attempting to obstruct a military draft after he distributed leaflets urging men not to submit).

decision of *Brandenburg v. Ohio*,[175] which is now considered the modern standard for determining whether incitement is deserving of First Amendment protection.[176] The case involved a Ku Klux Klan ("KKK") leader who was convicted for violating an Ohio criminal syndicalism law that punished those who "advocat[e] the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform" due to his participation in a KKK rally that was characterized as inciting in nature.[177] The Court overturned his conviction based on the notion that speech loses its protection only if "the advocacy is directed to producing imminent lawless action and is likely to incite or produce such action."[178]

While the *Brandenburg* doctrine remains in effect as the modern approach to classifying unprotected incitement, the Court has been stringent in its definition of imminence.[179] If the government fails to satisfy the *Brandenburg* test criteria, "content-based restrictions on political speech in a public forum" are evaluated under a strict scrutiny standard,[180] which is a very high burden for the government to meet.[181] This burden has proven to be difficult to satisfy, particularly when applied to issues involving free speech on the Internet, as the Supreme Court has been extremely consistent in awarding protections of expression in cyberspace.[182] Since the *Brandenburg* standard has not yet been applied to terrorist groups advocating for violence or religious

175. 395 U.S. 444 (1969).

176. Chris Montgomery, Note, *Can* Brandenburg v. Ohio *Survive the Internet and the Age of Terrorism?: The Secret Weakening of a Venerable Doctrine*, 70 OHIO ST. L.J. 141, 154-57 (2009). *Brandenburg* uprooted much of the case law created during the World War I and II eras. *Id.* at 154.

177. *Brandenburg*, 395 U.S. at 444-46; Pierce, *supra* note 175, at 259.

178. *Brandenburg*, 395 U.S. at 447. Here the defendant's words were not considered to have encouraged imminent violence. *See id.* at 448-49 ("[T]he mere abstract teaching of the . . . moral propriety or even moral necessity for a resort to force and violence, is not the same as preparing a group for violent action and steeling it to such action." (quoting Noto v. United States, 367 U.S. 290, 297-98 (1961))). The *Brandenburg* doctrine established a two-part test, which set forth criteria that the government must meet in order to prohibit certain forms of speech within constitutional boundaries. Gardella, *supra* note 119, at 674.

179. *See* R. Randall Kelso, *The Structure of Modern Free Speech Doctrine: Strict Scrutiny, Intermediate Review, and "Reasonableness" Balancing*, 8 ELON L. REV. 291, 328-30 (2016).

180. *Id.* at 329 (quoting Boos v. Berry, 485 U.S. 312, 321 (1983)). To survive strict scrutiny review, "the statute must: (1) advance compelling or overriding government ends; (2) be directly and substantially related to advancing those ends; and (3) be the least restrictive, effective means to advance those ends." *Id.* at 294.

181. Tony Mauro, *'Material Support' Ruling May Break 1st Amendment Ground*, FIRST AMEND. CTR. (June 22, 2010), http://www.firstamendmentcenter.org/material-support-ruling-may-break-1st-amendment-ground ("Strict scrutiny is usually fatal to government regulation of speech . . . .").

182. Gardella, *supra* note 119, at 675-77.

speech urging for jihad, it is unclear whether terrorist incitement on social media would be classified as unprotected for causing imminent violence.[183]

In 2010, the Supreme Court decided one of the most groundbreaking cases addressing international terrorism, where justices were forced to weigh the conflicting interests of national security and free speech.[184] *Holder v. Humanitarian Law Project*[185] marked the first time a statute has ever survived the Supreme Court's strict scrutiny standard in situations involving restraints on one's freedom of speech.[186] The statute in question was the Material Support Statute,[187] which was upheld in a six to three decision despite its consequential limitations on speech.[188] The Plaintiffs sought to provide support to two groups that they knew were deemed foreign terrorist organizations ("FTO"), by offering training to the groups' members on how to peacefully resolve conflicts and properly utilize representative bodies to petition and express their grievances.[189] They claimed that because they were only trying to assist the FTOs in achieving their nonviolent objectives, the application of the Material Support Statute deprived them of their freedoms of speech and association.[190] This argument failed as the Court deferred to Congress's prioritization of national security over unrestricted freedom of expression.[191] Chief Justice Roberts listed the potential threats to the country's national security that could arise from seemingly harmless assistance to known terrorist groups.[192] He also

183. Kelso, *supra* note 179, at 329-30. Some First Amendment scholars believe that speech advocating for terrorist violence to sympathizers willing to carry out attacks should sufficiently satisfy the imminence requirement. LEWIS, *supra* note 173, at 166-67. Those in support of this view often note that terrorist incitement is actually dangerous to the public, unlike the burning an American flag or making a racist remark, because it can lead to a mass attack with devastating effects. *Id.*

184. *See* Adam Liptak, *Justices Uphold a Ban on Aiding Terror Groups*, N.Y. TIMES, June 22, 2010, at A1; Mauro, *supra* note 181.

185. No. 08-1498, slip op. at 1 (June 21, 2010).

186. Mauro, *supra* note 181. The Court did not apply the *Brandenburg* standard in *Holder*. Kelso, *supra* note 179, at 330.

187. *Holder*, slip op. at 1; 18 U.S.C. §§ 2339A–2339B (2012).

188. Mauro, *supra* note 181.

189. *Holder*, slip op. at 2.

190. *Id.* at 2-3.

191. *Id.* at 36 ("Given the sensitive interests in national security and foreign affairs at stake, the political branches have adequately substantiated their determination that, to serve the Government's interest in preventing terrorism, it was necessary to prohibit providing material support . . . to foreign terrorist groups, even if the supporters meant to promote only the groups nonviolent ends."). The Court indicated that Congress carefully considered the restrictions that the Material Support Statute had on speech, which is why the statute excludes medicine and religious materials in its definition of "material support." *Id.*

192. *Id.* at 38.

acknowledged that this decision does impose slight restrictions on First Amendment rights,[193] but justified the decision on the premise that the Material Support Statute does not apply to "independent advocacy or expression of any kind," nor does it prevent or punish people for becoming members of an organization.[194] Therefore, plaintiffs were not barred from advocating the groups' legitimacy; they merely were prohibited from acting in coordination with designated FTOs, even if the support being provided was benign.[195] This decision has been classified as an indirect means for the government to circumvent First Amendment protections and demonstrated the Court's willingness to go to great lengths to curtail one of the greatest threats to humanity through the use of the Material Support Statute.[196]

IV. MEANS TO AN END: CURBING TERRORIST INCITEMENT ON SOCIAL MEDIA

Due to the vastness of its nature, managing terrorist incitement on social media has been referred to as a "gargantuan" task but it is not impossible with the guaranteed cooperation of social media platforms.[197] To ensure their participation, Subpart A first proposes an amendment to the CDA that would impose a "duty to take down" modeled after the DMCA, severing ISPs *complete* immunity under section 230.[198] However, in order to protect the government and these companies from constitutional claims that removal of a user's content violates a user's freedom of speech, there should be a more concrete distinction as to what terrorist incitement is protected and what must be removed within bounds of the First Amendment, as noted in Subpart B.[199] To safeguard one's right to freedom of expression as much as possible, as Subpart C

193. *See id.* at 27. Justice Roberts rejected the Government's argument that intermediate scrutiny should be applied because only conduct was at issue. *Id.* ("The Government is wrong that the only thing actually at issue in this litigation is conduct.").

194. *Id.* at 13, 23, 26 ("Individuals who act entirely independently of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction or control." (quoting 18 U.S.C. § 2339B(h) (2012))). The Court noted that it does not defer to the government's reading of the First Amendment, but does defer to the Legislature's "superior capacity" to weigh competing interests, especially with regard to terrorism. *Id.* at 36.

195. *See id.* at 27.

196. Barak-Erez & Scharia, *supra* note 47, at 19. Some scholars believe that the *Holder* decision actually strengthens the freedoms afforded by the First Amendment because it is not concerned with the content of the individual's speech. *See* Pierce, *supra* note 174, at 273-74.

197. *Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 63 (statement of Evan Kohlmann, Chief Information Officer, Flashpoint Partners).

198. *See infra* Part IV.A.

199. *See infra* Part IV.B.

explains, this duty seeks to impose only minimal restraints on speech that is already considered unprotected.[200]

A. Imposing a "Duty to Take Down" upon Notification of Inciting Material

The CDA currently provides almost automatic protection to ISPs for content posted by third parties.[201] In contrast, the DMCA creates an obligation for ISPs to take down copyright infringing materials upon notification of such content, and imposes liability for failing to do so.[202] This has led to a drastic difference in the ways that ISPs manage the unwanted content on their platforms, which is why Professor Ira Steven Nathenson has referred to the resulting implications of the two statutes as "the tale of two cities."[203] By imposing a "duty to take down" upon notification of terrorist incitement, social media companies will now be subject to limited liability for allowing the content to remain for public viewing only after becoming aware of such material.[204]

Currently, the DMCA is the only federal legislation in the United States that establishes a "duty to take down" content that is not explicitly proscribed by criminal law.[205] According to section 512(c)(1)(A) of the DMCA, a service provider is entitled to safe harbor protection with regard to infringing material only if it:

> (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.[206]

In contrast, section 230 of the CDA states that "No provider or user of an [ISP] shall be treated as the publisher or speaker of any information provided by another information content provider."[207] In order to ensure the cooperation of social media companies and other ISPs hosting online forums abused by terrorists, a duty for ISPs to take down the incitement on their platforms must be created.[208] Since it has

200. *See infra* Part IV.C.
201. *Paris Victim's Father Sues Twitter, Facebook, Google over ISIS*, *supra* note 137.
202. 17 U.S.C. § 512(c)(1) (2012).
203. Nathenson, *supra* note 21, at 110-12.
204. *Cf.* 17 U.S.C. § 512(c)(1).
205. *See* RUSTAD & KOENIG, *supra* note 16.
206. 17 U.S.C. § 512(c)(1)(A).
207. 47 U.S.C. § 230(c)(1) (2012).
208. *See supra* Part III.B.

already been established that no one shall knowingly provide "material support" to a designated FTO, the liability should be imposed based on whether an ISP had knowledge that a member of a FTO, or person working in coordination, is using its platform.[209] Therefore, section 230(c)(1) of the CDA should be amended as follows:

> (c)(1) No provider or user of an interactive service provider shall be treated as the publisher or speaker of any information provided by another information content provider, *except as provided in subsection (A).*[210]
>
> *(A) EXCEPTION – An Internet Service Provider shall not knowingly provide its services to any member of or person acting in coordination with a foreign terrorist organization*[211] *pursuant to 18 U.S.C. § 2339A.*[212] *An Internet Service Provider may be treated as publisher or speaker of any information provided by another content provider that is a member of or a person acting in coordination with a foreign terrorist organization if the Internet Service Provider:*
>
> *(i) has actual knowledge that the content was posted by a member of a foreign terrorist organization or a person working in coordination with a foreign terrorist organization; or*[213]
>
> *(ii) upon obtaining such knowledge or awareness, fails to act expeditiously in removing or disabling the user's account.*[214]

The Material Support Statute classifies "communications equipment" given to a FTO or its individual members as a form of "material support" that is explicitly prohibited under the statute.[215] Financial institutions that become aware that they have possession of any funds belonging to a FTO are instructed not to disperse the funds to

---

209. *See supra* Part III.C.

210. 47 U.S.C. § 230(c)(1).

211. 8 U.S.C. § 1189 (2012). Currently, the U.S. Department of State has designated sixty-one terrorist organizations as FTOs. *See Foreign Terrorist Organizations*, DEP'T STATE, https://www.state.gov/j/ct/rls/other/des/123085.htm (last visited Aug. 1, 2017).

212. 18 U.S.C. § 2339A (2012). While ISPs, in theory, are still subject to liability according to federal criminal law, recent case law has indicated that ISPs tend to enjoy blanket immunity with regard to the Material Support Statute. 47 U.S.C. § 230(e)(1); *see supra* Part III.A. It is therefore necessary to explicitly note the Material Support Statute's application when imposing a duty to take down.

213. *See* 17 U.S.C. § 512(c)(1)(A) (2012); 18 U.S.C. § 2339B(1); Holder v. Humanitarian Law Project, No. 08-1498, slip op. at 1, 11, 16-17 (June 21, 2010) ("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.").

214. *See* 17 U.S.C. § 512(c)(1)(A)(i)–(iii); 18 U.S.C. § 2339B.

215. 18 U.S.C. § 2339A(b)(1); *see, e.g.*, Benjamin Weiser, *S.I. Man Gets Prison Term for Aid to Hezbollah TV*, N.Y. TIMES, Apr. 24, 2009, at A22 (discussing the criminal conviction of a man accused of providing communications equipment to Hezbollah by providing the FTO satellite services, allowing the FTO to broadcast its channel to viewers in New York City).

the FTO and must report to the Secretary of State.[216] If a financial institution fails to comply with the statute's requirements once it learns that it has been providing material support to a designated FTO, it may become subject to a civil penalty of $50,000 per violation.[217] Similarly, an ISP that receives notification of terrorist activity on its platform becomes aware that it is providing communications equipment to a FTO or those working in coordination with one will now have a duty to take down the account under the proposed amendment of the CDA.[218] Like financial institutions, legislators may choose to hold ISPs civilly liable under the Material Support Statute so that they have a legal incentive to remove terrorist incitement on their platforms.[219]

In order for ISPs to learn that terrorists belonging to, or working with, a FTO are utilizing their platforms, some sort of specialized reporting entity must be established so that ISPs know to take action.[220] Organizations dedicated to counterterrorism, such as the CEP have suggested that social media companies grant "trusted reporting status" to law enforcement agencies and like-minded organizations that would help ISPs identify and remove terrorists utilizing their platforms.[221] The Obama Administration had blessed the collaboration of social media giants and the CEP's National Office for Reporting Extremism, which was launched to assist social media companies in addressing terrorist incitement on their platforms.[222] Its role would be similar to that of the National Center for Missing and Exploited Children, which currently works with social media companies to detect and quickly remove child pornography shared on their sites.[223] However, unlike private companies who are free from First Amendment considerations when creating their own grounds for removal, government agencies are still bound by the First Amendment and should not have unlimited discretion in determining what shall be removed.[224] This is why it is necessary to define what constitutes unprotected terrorist incitement, which the next Subpart discusses.[225]

---

216. 18 U.S.C. § 2339B(a)(2).

217. *Id.* § 2339B(b)(A).

218. *See supra* notes 208-15 and accompanying text.

219. *See* Davis, *supra* note 70, at 160-62.

220. *See, e.g.*, *Digital Disruption Fighting Online Extremism*, COUNTER EXTREMISM PROJECT, http://www.counterextremism.com/digital-disruption (last visited Aug. 1, 2017).

221. *Id.*

222. Nakashima, *supra* note 16.

223. *Id.*

224. Citron & Norton, *supra* note 157, at 1439 & nn.20-24.

225. *See infra* Part IV.B.

B. *Defining Unprotected "Terrorist Incitement" in the Interest of Free Speech*

The notion of imposing a "duty to take down" has been controversial to many, especially for social media companies that are currently enjoying complete immunity provided by the CDA.[226] One of the primary objections in response to the proposal of creating a "duty to take down" terrorist incitement from an ISP's perspective is that there is a lack of consensus as to what constitutes terrorist incitement.[227] In order for the "duty to take down" proposed in Subpart A to work,[228] social media companies must be given guidance as to what content involving terrorism should and should not be permitted on their platforms.[229] Unlike child pornography, in which the photograph itself is inherently illegal, speech promoting terrorism is not as easily defined.[230]

In defining what constitutes unacceptable terrorist incitement on social media, the government must be careful to respect the boundaries of the First Amendment.[231] While the Court emphasized in *Holder* that its decision was limited to the facts of this specific case and would not be indicative of the outcome of every circumstance involving the support of terrorist groups, the Court demonstrated that limiting one's freedom of speech does not always serve as a constitutional violation if that speech is coming from a FTO or its affiliates.[232] To reiterate, the Court noted that in order for an act to constitute "material support" in violation of the Material Support Statute, it must be "coordinated with or under the direction of a foreign terrorist organization," meaning that an individual's "[i]ndependent advocacy that might be viewed as promoting the group's legitimacy is not covered."[233] Based on this premise, terrorist incitement should be defined as anything posted by a user who is known to be a member of a designated FTO or who is known to be acting in coordination with one, for purposes of mandatory removal.[234]

---

226. *See, e.g.*, Gardella, *supra* note 119, at 682-83 (arguing that holding ISPs accountable for content on their platforms threatens the functionality of the Internet and would chill Internet activity altogether); *Infographic: Why the CDA Is So Important*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/cda230/infographic (last visited Aug. 1, 2017); Nakashima, *supra* note 16.

227. Nakashima, *supra* note 16.

228. *See supra* Part IV.A.

229. Nakashima, *supra* note 16. ISPs are free to determine their own standards through their "Terms of Service" as to what justifies grounds for removal that exceed the minimum standard of unprotected speech set forth by the government. Paslawsky, *supra* note 109, at 1496-97.

230. Nakashima, *supra* note 16.

231. *See supra* Part III.C.

232. Holder v. Humanitarian Law Project, No. 08-1498, slip op. at 1, 8 (June 21, 2010).

233. *Id.* at 26.

234. *See id.* at 1, 8; Wittes & Bedell, *supra* note 130.

It is important to note that in order to pass constitutional muster, the grounds for removal here are not based on the nature of what the terrorist is actually posting, but the fact that a member of a designated FTO is using the platform in general.[235] Since the Material Support Statute does not apply to independent speech, an independent user exclaiming, "I believe ISIS is justified in its use of terrorism to achieve its objectives" or "Al-Qaeda is the best" would be protected.[236] On the other hand, a user who is known to belong to ISIS or Al-Qaeda should not be using the platform at all and must be removed, even if he is merely posting pictures of puppies or recipes for his favorite meal.[237] While this may seem counterintuitive at first glance, the reality is that members of designated FTOs are usually not sharing photos of animals or the food that they are eating, but instead are posting videos of beheadings and sermons online that have inspired a number of homegrown terror attacks in the United States.[238]

One of the problems that counterterrorism experts encounter is that many terrorists utilizing social media do so from an anonymous account or post through a pseudonym to disguise their identity.[239] This does make it more difficult to decipher whether a user is a member of a designated FTO; however, there are still many terrorists belonging to FTOs that do not disguise themselves and openly post terrorist propaganda on the group's behalf.[240] For example, many terrorist groups have multiple accounts on Twitter that post in English and can be easily traced by the general public, including, but not limited to, Hamas, Hezbollah, Popular Front for the Liberation of Palestine, Ansar al-Islam, and the Kurdistan Workers' Party.[241] Videos produced by terrorist organizations often include a group's signature to indicate to viewers

235. Wittes & Bedell, *supra* note 130.

236. *See id.*

237. *See id.*

238. *See id.* (noting that Twitter would violate the Material Support Statute if it was aware of any tweets posted by ISIS, including innocent tweets containing videos of cats); *see also supra* Part II.C. A social media account called the "Cats of Jihad" does exist, which allows ISIS members to post pictures of their cats posing with weapons. P.W. Singer & Emerson Brooking, *Terror on Twitter*, POPULAR SCI. (Dec. 11, 2015), http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media. Should the CDA be amended as Part IV.A of this Note suggests, the "Cats of Jihad" account would need to be removed if it were run by a member of a designated FTO, but could remain if it were an independent person acting on his own volition. *See supra* notes 230-36 and accompanying text.

239. *See, e.g.*, *Hearings on Jihadist Use of Social Media*, *supra* note 80, at 6 (statement of William F. McCants, Analyst, Center for Naval Analysis) (noting that Al-Qaeda members often remain anonymous when sharing inciting material).

240. *See* Singer & Brooking, *supra* note 238.

241. Bedell & Wittes, *supra* note 130.

which group produced the video.[242] Some terrorist groups orchestrate their own public question-and-answer sessions through online discussion boards or through the use of hashtags, such as "#AskHamas."[243] Should a "duty to take down" be imposed, once a reporting entity notified ISPs of FTO presence on their platforms, ISPs would be required to terminate all of the previously mentioned social media presence, and would be subject to civil liability for failing to do so expeditiously.[244]

C. Addressing the Arguments of Those who Support Complete Immunity for Internet Service Providers

Similar to those who criticize the DMCA's imposition of a "duty to take down" for its subsequent restrictions on free speech, civil liberties advocates and those that seek unrestricted expression in cyberspace will likely have the same concerns with the creation of a "duty to take down" terrorist incitement under an amended CDA.[245] First, staunch supporters of the CDA often profess fears of overzealous censorship.[246] For example, the Electronic Frontier Foundation cites "real life examples" of countries that do not employ safe harbor protections under the CDA, such as legislation passed in Thailand that holds ISPs criminally responsible for posts by users that speak critically of the royal family of Thailand on their platforms.[247] However, this would never happen in the U.S. because case law shows that the First Amendment explicitly prohibits the use of such content-based limitations on speech.[248]

Opponents to the establishment of a "duty to take down" related to defamation and privacy norms under the CDA claim that ISPs will opt to voluntarily take down borderline material that would be considered protected under the First Amendment in order to avoid the risk of litigation resulting from its failure to remove the offending content.[249] Civil liberties advocates will likely assert that the proposed amendment to the CDA will result in excessive censorship of incitement on social media, even if the material is not in reality posted by a member of a

242. *Hearings on Jihadist Use of Social Media*, *supra* note 80, at 9 (statement of Andrew Aarom, Director, Society for Internet Research).

243. Bedell & Wittes, *supra* note 130; Singer & Brooking, *supra* note 238.

244. *See supra* Part IV.A.

245. *See* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J. L. & TECH. 171, 193-97 (2010).

246. *See, e.g.*, *Infographic: Why the CDA is So Important*, *supra* note 226.

247. *Id.*

248. *See supra* Part III.C.

249. Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET 25 (Saul Levmore & Martha C. Nussbaum eds., 2010).

FTO.[250] It is important to note, however, that social media companies already enjoy the ability to remove content based on their own self-imposed standards, as private entities are not bound by the restrictions of the First Amendment.[251] In fact, entrusting a government entity with "trusted reporting status" when notifying ISPs of FTO use of their platforms would actually impose a minimum standard of First Amendment protection since the ISPs will have a duty to comply with the government's request.[252] As the Court provided in *Holder*, cases involving the Material Support Statute may still be subject to judicial review if a party feels that its First Amendment rights were violated.[253]

Lastly, groups supporting ISPs' blanket protection under section 230 note that the costs for operating online platforms will increase, and could potentially spread to ISP users so that social media will no longer be free of charge.[254] They argue that ISPs will need to hire more lawyers to review content and fight lawsuits brought by users, and will have to pay additional financial damages if courts start to rule in favor of plaintiffs suing ISPs for allowing incendiary material on their platforms.[255] However, the proposed amendment would only satisfy the requirement that an ISP "knowingly" provides material support to a FTO if the ISP was notified of the FTO's presence and failed to remove the content.[256] Plaintiffs in suits like *Gonzalez* and *Fields* suing ISPs must still prove that the ISP knew the content posted came from a member of a designated FTO, or someone acting in coordination with a FTO, and would also have to overcome the difficult hurdle of proving causation between the incitement and the injuries caused as a result of an act of terror.[257] There is no way to predict whether ISPs would begin to charge its users seeking to utilize their services to compensate for the additional costs incurred from increased litigation, but if that were the case, the general public may find it to be a price worth paying to ensure their own safety from the spread of new terrorism.[258]

---

250. *See* Seth Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, & the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 29-31 (2006) (arguing that allowing intermediaries to make censorship decisions poses the risk of "veto on the speech of others").

251. Citron & Norton, *supra* note 157, at 1439. Many of the leading social media platforms already contain prohibitions against terrorist incitement in their "Terms of Service." *See supra* note 17 and accompanying text.

252. *See supra* Part III.C.

253. Holder v. Humanitarian Law Project, No. 08-1498, slip op. at 1, 35-36 (June 21, 2010).

254. *See, e.g.*, *Infographic: Why the CDA Is So Important*, *supra* note 226.

255. *Id.*

256. *See supra* Part IV.A.

257. *See supra* Part III.A.

258. *See Views of Governments Handling of Terrorism Fall to Post 9/11 Low*, PEW RES. CTR. (Dec. 15, 2015), http://www.people-press.org/2015/12/15/views-of-governments-handling-of-

V. CONCLUSION

It is unrealistic to think that curbing terrorists' use of social media will completely eradicate the spread of terrorist propaganda on the Internet.[259] However, imposing a duty to take down content posted by a foreign terrorist organization is a first step to alleviating a problem that will continue to grow if it is not properly managed.[260] Experts often note that, in order for a terrorist movement to be successful, it must be able to maintain relevance, induce morale, and recruit new members.[261] By limiting terrorists' use of social media, the reach of their propaganda will diminish, making it more difficult for ISIS, Hamas, Al-Qaeda, and other terrorist groups to accomplish their goals.[262] Although this does expose social media companies to potential liability, the duty proposed is very limited in scope and compliance may make it more difficult for terrorist organizations to communicate with each other and the general public, potentially saving many lives.[263]

*Michelle Roter**

terrorism-fall-to-post-911-low (citing a 2015 study that showed that 56% of the American population feels the government has not gone far enough in their efforts to protect the country from terrorists). This same study revealed that 28% of the population currently feels that the government's anti-terrorism policies have gone too far in restricting citizens' civil liberties, the lowest reported number since the September 11, 2011, attacks. *Id.*

259. *See Hearings on the Evolution of Terrorist Propaganda*, *supra* note 13, at 42-45 (statement of J.M. Berger, Nonresident Fellow, the Brookings Institution) (comparing managing terrorist incitement on social media to gardening weeds in that both require constant upkeep).

260. *See id.*

261. *See Hearings on Jihadist Use of Social Media*, *supra* note 80, at 11 (prepared statement of Andrew Aaron Weisburd, Director, Society for Internet Research).

262. Greenberg, *supra* note 159.

263. *See supra* Part IV.

* J.D. Candidate, 2018, Maurice A. Deane School of Law at Hofstra University; B.A., 2014 Binghamton University. First, I would like to thank my parents, Cindy and Gil Roter, for their endless love and support throughout my life, but especially while in law school. A huge thank you to my brother, Adam Roter, who has served as a constant source of encouragement and comic relief during times of great stress. I would also like to thank my Faculty Advisor, Irina Manta, for her time and assistance over the past year. To my Notes Editor, Ashley Flynn, I could not have asked for a better mentor to guide me through the Note writing process. I am also extremely grateful to Joseph De Santis, Michelle Malone, Susan Loeb, Jonathan DeMars, Tessa Patti, Mindy Hollander, Omar Abdelkader, Alexis Fallon, Carolyn McNamara, and the rest of Volume 45, without whom this publication would not be possible. Finally, I would like to thank my best friend, Taylor Pugliese, for being by my side every step of the way, starting from the very first day of law school orientation.

***

***