TERROR ON THE INTERNET: COMPARING THE UNITED STATES AND EUROPEAN UNION SOCIAL MEDIA REGULATIONS TO PREVENT TERRORISM

MADELINE SCHNEIDER*

INTRODUCTION

Margaret Thatcher once "referred to publicity as the oxygen on which terrorists depend."[1] This relationship between publicity and terrorism has only strengthened with each passing year. In 2002, America was horrified by the videotaped murder of Daniel Pearl, an American journalist. The video was recorded on a "camcorder and initially distributed by videotape."[2] However, the circulation of the video was limited to only those who were affiliated with the terror group. In 2014, another American journalist, James Foley, was brutally murdered on video by members of the Islamic State, otherwise known as ISIS.[3] The ISIS member warned President Barack Obama that more American blood would be spilled with every American attack on ISIS.[4] The video ended with the terrorist stating, "'[T]he life of this American citizen, Obama, depends on your next decision.'"[5] The video was posted on social media with the hashtags "#A_Message_To_America and #NewMessageFromISIStoUS."[6] The video "amassed more than 2,000 tweets in the first three hours of the [it's] release . . . more than 80 percent of adults in Great Britain knew about the video of Foley's murder within days of it being posted online."[7] Unlike the limited audience of the Pearl video, the advent of social media has made circulating these gruesome videos easier. ISIS has built its name "on the marketing of savagery, evolving its message" through social media using "carefully manipulated version[s] of its

---

* J.D. candidate for 2021 at Indiana University's McKinney School of Law and has a bachelor's degree in International Affairs from the University of Cincinnati.

1. Jessica Stern, *The War Against Terror Must Be Fought with Words Too*, TIME MAG. (Dec. 16, 2013), https://ideas.time.com/2013/12/16/the-war-against-terror-must-be-fought-with-words-too/ [https://perma.cc/9THX-UYJW].

2. Adam Taylor, *From Daniel Pearl to James Foley: The Modern Tactic of Islamist Beheadings*, WASH. POST (Aug. 20, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/08/20/from-daniel-pearl-to-james-foley-the-modern-tactic-of-islamist-beheadings/ [https://perma.cc/C8ZP-TFCN].

3. JESSICA STERN & J.M. BERGER, ISIS: THE STATE OF TERROR 1 (2015) [hereinafter ISIS: THE STATE OF TERROR]; Megan Specia, *The Evolution of ISIS: From Rogue State to Stateless Ideology*, N.Y. TIMES (Mar. 20, 2019), https://www.nytimes.com/2019/03/20/world/middleeast/isis-history-facts-islamic-state.html [https://perma.cc/Y35L-QLHG].

4. ISIS: THE STATE OF TERROR, *supra* note 3, at 1.

5. *Id*. at 5.

6. Zann Isacson, *Combating Terrorism Online: Possible Actors and Their Roles*, LAWFARE (Sept. 2, 2018, 10:00 AM), https://www.lawfareblog.com/combatting-terrorism-online-possible-actors-and-their-roles [https://perma.cc/7529-K7SY].

7. *Id*.

military campaigns" and videos like Foley's.[8] On March 15, 2019, the way terrorists used social media became even more complex. In New Zealand, fifty people were killed, and many more were injured when a gunman entered two mosques and opened fire.[9] The entire massacre was live-streamed on Facebook. During the live stream, "fewer than 200 people had watched it live," and it was not reported until twelve minutes after it ended.[10] However, "within 24 hours, [Facebook] had blocked 1.2 million copies at the point of upload," and it was viewed more than 4,000 times before it was removed. [11] Months after the attack, Facebook was still fighting to remove the video and related content.[12] So far, it has removed 4.5 million copies and posts related to the terror attack.[13] The birth of social media has transformed and expanded the way terrorist groups communicate and spread their propaganda. The current leader of Al Qaeda has said, " we are in a battle, and that more than half of this battle is taking place in the battlefield of the media."[14]

Social media provides terror groups with a global stage. Just as everyday Americans enjoy the interconnectedness and ease of social media, terrorist groups do as well. Before social media and the mass internet, it was more difficult for terror groups to spread their message and recruit members. They used terror attacks to gain attention and spread their message. Face-to-face contact was used to recruit members, limiting recruitment to those who had connections with terror groups. Social media provides a cheap and easy means to reach members and potential recruits alike. "The Internet offers the means to connect with vast groups of people, overcoming traditional geographic constraints."[15] In a hearing before the House Subcommittee on National Security in 2015, this transcendence of borders was highlighted:

> While foreign fighters travel overseas for training and to make other terrorist connections, it's becoming apparent that Islamic recruits in the United States and other parts of the world who are unable to travel to these battlegrounds do not necessarily need to do so in order to receive

---

8. ISIS: THE STATE OF TERROR, *supra* note 5, at 3.

9. *Facebook: New Zealand Attack Video Viewed 4,000 Times*, BBC NEWS (Mar. 19, 2019), https://www.bbc.com/news/business-47620519 [https://perma.cc/7RT7-FNT9].

10. *Id.*

11. *Id.*

12. David Uberti, *The Christchurch Terror Attack Video is Still Spreading on Facebook*, VICE NEWS (Nov. 13, 2019), https://www.vice.com/en_us/article/wjw93n/the-christchurch-terror-attack-video-is-still-spreading-on-facebook [https://perma.cc/SX7X-GAZC].

13. *Id.*

14. Eric V. Larson, *Al Qaeda's Propaganda: A Shifting Battlefield*, *in* THE LONG SHADOW OF 9/11: AMERICA'S RESPONSE TO TERRORISM 71, 84 (Brian Michael Jenkins & John Paul Godges eds., 2011).

15. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR.: WHAT EVERYONE NEEDS TO KNOW 99-100 (2014); *see also* MARTHA CRENSHAW & GARY LAFREE, COUNTERING TERRORISM 170 (2017) (ebook).

> training and inspiration. They can engage real time with jihadists on Twitter, watch ISIS's murderous propaganda on YouTube, view jihadi selfies on Instagram, or read religious justifications for the killing of civilians on Just Paste It.[16]

People with similar interests are now able to form groups and share information where they otherwise would not be able to. Social media allows one person's voice "to be magnified and reach more people."[17] One person, without much effort, can now reach millions of people from all over the globe. "Today, 90 percent of terrorist activity on the Internet takes place using social networking tools."[18] Social media allows "subscribers a chance to make direct contact with terrorist representatives, to ask questions, and even to contribute and help out the cyberjihad."[19]

The advantage of social media is twofold: it is an all-in-one platform; it is the stage, the audience, and the voice. The internet also provides a level of anonymity and a lack of attribution. "These forums act as a virtual firewall to help safeguard the identities of those who participate."[20] The anonymous aspect of Internet use is valuable to terror organizations. They can now "obscure their operations in new ways that complicate the old ways of thinking about threats."[21] For example, the Taliban "ran a propaganda website for over a year that kept a running tally of suicide bombings and other attacks against American troops in Afghanistan."[22] The website was hosted by a Texas company called ThePlanet. The company was unaware of the Taliban's website until the authorities alerted them.[23] This level of anonymity proves to be a challenge for anyone engaged in counterterrorism.

The non-traditional aspect of social media presents countries with a unique problem. Unlike the more traditional modes of communication where only a small number of established news organizations disseminate information, social media enables anyone to publish or access information and to do so in an interactive, two-way exchange."[24] The unprecedented speed at which terrorists can reach and radicalize people has created difficulties in fighting the dissemination of terrorist content.[25] Countries around the world have taken

---

16. *Radicalization: Social Media and the Rise of Terrorism: Hearing before the Subcommittee on Nat'l Sec. of the H. Comm. On Oversight & Gov't Reform*, 114th Cong. 2 (2015) [hereinafter *Radicalization: Social Media and the Rise of Terrorism*] (statement of Former Rep. Ron DeSantis, Chairman, Subcomm. on Nat'l Sec.).

17. SINGER & FRIEDMAN, *supra* note 15, at 99.

18. Gabriel Weimann, *Terrorist Migration to Social Media*, 16 GEO. J. INT'L AFFAIRS 181 (2015).

19. *Id.*

20. *Id.*

21. SINGER & FRIEDMAN, *supra* note 15, at 103.

22. *Id.*

23. *Id.*

24. Weimann, *supra* note 18, at 181.

25. *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 19, at 2.

varying degrees of approaches to combat this modern threat. The European Union has taken steps toward passing a law that regulates the content on social media. This proposed law, known commonly as the Terrorist Content Regulation, aims to tackle the dissemination of terrorist propaganda through referral systems.[26] This regulation places most of the burden on the private social media company to combat terrorist propaganda, with financial penalties for discontinued failures to remove flagged content.[27]

The United States, by contrast, has yet to pass such a comprehensive and all-encompassing law. Unlike the European Union and other countries that have comprehensive counterterrorism laws, the United States must contend with the Constitution. In passing laws regulating the content that is allowed on social media, the United States government must make sure that it does not abridge free speech. Keeping this in mind, American commenters have looked to existing United States laws to help curb the influx of terrorist content online. One of these laws is 18 U.S.C. 2339(B). This is a material support statute that makes people either criminally or financially liable for providing material support to terrorist organizations.[28] However, this law and others have proved ineffective in certain cases where tech companies can invoke Section 230 of the Communications Decency Act. This Act provides immunity for tech companies against lawsuits regarding the posts of their users.[29] In recent years, this law has become the ultimate trump card for tech companies involved in lawsuits involving terrorist content, among other things. Section 2339(b) has been proposed to hold tech companies liable for terrorist content. These two laws could be used to fight online terrorist propaganda. In a hearing before the House Subcommittee for National Security, former Representative Ron DeSantis stated: "In order to combat this trend, we must ensure that law enforcement has the necessary tools to do its job. Efforts to counter and deter unconventional information warfare must be joined with other government agencies' efforts to deal with the problem of terror on social media."[30]

In Part I, this Note will look at the European Union's current Internet Forum and their proposed Terrorist Content Regulation. The proposed regulation focuses

---

26. Jon Porter, *Upload Filters and One Hour Takedowns: The EU's Latest Fight Against Terrorism Online, Explained*, THE VERGE (Mar. 21, 2019), https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu [https://perma.cc/62RF-ZPU7]; *see generally Commission Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*, at 1, COM (2018) 640 final (Dec. 12, 2018) [hereinafter *Commission Proposal*]; *see also* R*eport on the Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online* (Apr. 9, 2019), https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2019/0193/P8_A(2019)0193_EN.pdf [https://perma.cc/7FGC-2MLJ] [hereinafter *Report on Commission Proposal*].

27. Porter, *supra* note 26; *see generally* EUR. PARL. DOC. (COM 0640) (2019).

28. 18 U.S.C. § 2339(B) (2019).

29. 47 U.S.C. § 230 (2019).

30. *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 16, at 3.

on countering terrorist content on social media by placing much of the burden on the social media companies themselves. This is unlike anything the United States currently has, and this proposal could be used to guide future American counterterrorism policies on social media. Next, this Note will turn to look at current American laws that may be used to combat terrorist propaganda online. Part II will focus on the Material Support of Foreign Terrorist Groups Statue: 18 U.S.C. § 2339(b). This statute creates liability for those who materially support organizations that are designated as foreign terrorist organizations. It has been proposed to help hold social media companies responsible for terrorist content on their platforms. In Part III, this Note will look at Section 230 of the Communications Decency Act. This law is not a counterterrorist or anti-terrorism law. Instead, this law protects social media companies from liability due to the content that their users post. This law has been crucial in many private lawsuits against social media companies for having terrorist content on their platforms.

These laws all have benefits in preventing the dissemination of terrorist content. However, as this note will discuss, the best way to prevent terrorist content while also preventing an "overstep" by the private and federal governments is to create an exception within the Communications Decency Act; that is conditioned upon social media companies' failure to act after being alerted to potential terrorist content. This Note proposes two conditions or "chances," the first one being, the social media company identifies the content themselves and takes measures to remove it. The second, and final chance, is that law enforcement alerts the company to terrorist content. This recommendation combines some aspects of the EU's Internet Forum and the proposed EU Terrorist Content Regulation.

BACKGROUND

A. Coercion Through Terror

Terrorism is not a new phenomenon. For thousands of years, "terrorists have wrought destruction in furtherance of religious or secular ends."[31] Many people in the United States view terrorism as a modern occurrence. However, American history has many incidents of terrorist attacks: "from presidential and other political assassinations to Civil War-related terrorist violence . . . our nation has experienced its share of lethal and usually politically-motivated terrorism." [32] Although, it has only been in recent decades that terrorism has taken center stage in America's national security interests.

The end of the Cold War brought an end to the threat of nuclear war and mutually assured destruction. The world stage was no longer defined by its

---

31. STEPHEN DYCUS ET AL., COUNTERTERRORISM LAW 4 (3rd ed. 2016); *see generally Module 1: Introduction to International Terrorism*, U. N. OFF. ON DRUGS AND CRIME (2018), https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf [https://perma.cc/7Y86-PBT7].

32. *Id.*

bipolarity. The struggle between the United States and the U.S.S.R. had ended, leaving behind a structured world where one's enemies were clear and national security was set on one goal. The new world order was much different. There was a new threat emerging: international terrorism.[33] Since the end of the Cold War, "the conventional wisdom that terrorists employed violence in discriminate and proportionate ways was called into question."[34] The first indication that these terrorists were departing from their old ways was that they "did not necessarily espouse political causes or aim to take power."[35] "Instead of kidnapping an ambassador, the 1990s-vintage terrorists took a whole embassy hostage.[36] Rather than hijack an aircraft, terrorists plotted to blow planes out of the sky."[37] These horrific acts presented countries with a range of new military tactics and foreign policy issues. The 1990s saw a change in how terrorists were working.[38] They had "upped the ante from pipe bombs to truck bombs capable of blowing up entire buildings."[39] The constraints that had confined the terror groups of the 1970s and 1980s were no longer present in the ranks of terror groups of the 1990s.[40] As the more restrained or "squeamish dropped out" and the "need for more news headlines demanded higher body counts."[41] These were no longer small-scale acts that were aimed at gaining political control. Terrorists were "intent on harming [the] maximum number of people" but are now contemplating attacks that could harm tens of thousands of civilians.[42]

B. Why is Terrorism Hard to Define?

At first glance, terrorism might look easy to define. In theory: "it's an unlawful use or threat of violence against persons or property to further political or social objectives."[43] When it comes to defining terrorism in practice, the task gets much harder. Most of the problem comes from the struggle of defining "the meaning or illegality of 'terrorism.'"[44] A terrorist act is easier to describe rather than to define because it is not a "conceptually clean label."[45] As with most

---

33. *Id.*

34. *Id. See also* Brian Michael Jenkins, *The New Age of Terrorism*, *in* MCGRAW-HILL HOMELAND SECURITY HANDBOOK: STRATEGIC GUIDANCE FOR A COORDINATED APPROACH TO EFFECTIVE SECURITY AND EMERGENCY MANAGEMENT 118 (2nd ed. 2012).

35. DYCUS ET AL., *supra* note 31, at 4.

36. *Id.*

37. *Id*; *see also* Jenkins, *supra* note 34, at 124.

38. Jenkins, *supra* note 34, at 118.

39. STEPHEN DYCUS ET AL., *supra* note 31, at 4.

40. Jenkins, *supra* note 34, at 118.

41. *Id.*

42. DYCUS ET AL., *supra* note 31, at 4.

43. *Id.* at 1.

44. *Id.* at 4.

45. *Id.* at 1; Jenkins, *supra* note 34, at 118; Tom Parker & Nick Sitter, *The Four Horsemen of Terrorism: It's Not Waves, it's Strains*, 28 TERRORISM & POL. VIOLENCE 197, 211 (Dec. 17,

things, the very definition of terrorism has become politicized, "because polemicists have used the term in a variety of self-serving ways over the years 'terrorism' might be applied today to describe any disfavored action taken in response to another's policies."[46] Instead of using a set of objective criteria, many uses "subjective interpretations of the term 'terrorism' [and also] the more generic appellation 'violent extremism.'"[47] To separate themselves from President Bush's administration, President Obama's administration used the ambiguous term "violent extremism."[48] The idea of who is a terrorist can be subjective. For one country or leader, a group of insurgents are terrorists. However, for the people in that group, they are freedom fighters. Due to its subjective nature, "the cliché that 'one man's terrorist is another man's freedom fighter' lives on."[49] This commonplace cliché only complicates the debate by confusing the ends with the means.[50] Terrorism can serve different political agendas or actors, and it is not necessarily tied to one group or ideology.[51]

This is further complicated by the sheer difference in the types of people or motivations that fall under the umbrella of terrorism: freedom fighters, religiously or racially motivated groups, insurgents, or guerilla groups.[52] Terrorist organizations "come in many different shapes and sizes, and they evolve and mutate."[53] They are complex actors that may wear multiple different identities—"terrorist and freedom fighter, terrorist and revolutionary."[54] Countries like Egypt or Bahrain might intentionally use a broad definition of terrorism, one that includes "legitimate political dissenters."[55]

The amorphous nature of terrorism is one of the reasons that there is no internationally accepted definition of terrorism. This results in definitions that are too broad or too narrow. In the nineteenth century, the definition of terrorism was: "propaganda of the deed."[56] In other words, a political message is better communicated to the masses through an act of violence rather than a pamphlet.[57] This definition encapsulates the one aspect of terrorism, which is to "shock and surprise" in order to reach the maximum number of people.[58] The complex nature and identities of terrorist organizations, while hard to articulate, can all be said

---

2015).

46. DYCUS ET AL., *supra* note 31, at 5.
47. CRENSHAW & LAFREE, *supra* note 15, at 16.
48. *Id.*
49. DYCUS ET AL., *supra* note 31, at 26.
50. CRENSHAW & LAFREE, *supra* note 15, at 16.
51. *Id.*
52. DYCUS ET AL., *supra* note 31, at 5.
53. Parker & Sitter, *supra* note 45, at 211.
54. *Id.*
55. ISIS: THE STATE OF TERROR, *supra* note 3, at 133.
56. CRENSHAW & LAFREE, *supra* note 15, at 17.
57. Parker & Sitter, *supra* note 45, at 199; *see also* CRENSHAW & LAFREE, *supra* note 15, at 17.
58. CRENSHAW & LAFREE, *supra* note 15, at 17.

to have one thing in common: "they are all prepared to indiscriminately and violently target civilians for political gain."[59]

The United States has attempted to solve the ambiguous nature of defining terrorism when they drafted 18 U.S.C. § 2331. Instead of focusing on what terrorism is, as a whole, the drafters listed terrorist activities along with motivations. This way, it can avoid the common pitfall of an overly broad or narrow definition that some countries have experienced. Together these lists combine to create one comprehensive list that provides better parameters for law enforcement. The statute lists terrorist activities as "violent acts or acts dangerous to human life" that appear or are intended "(1) to intimidate or coerce a civilian population; (2) to influence the policy of a government by intimidation or coercion; or (3) to affect the conduct of a government by mass destruction, assassination, or kidnapping."[60] Another interesting aspect of the statute is that it doesn't limit terrorism to a person, it defines a "person" as "any individual or entity capable of holding a legal or beneficial interest in the property."[61] In addition, the statute makes a distinction between international and domestic terrorism. The difference lies in whether the act occurred in the United States or it "transcended national boundaries in terms of the mean by which they are accomplished."[62]

I. THE EUROPEAN UNION'S APPROACH: THE PROPOSED TERRORIST CONTENT REGULATION

The United States is not alone in the fight against terrorism. Europe saw a spike in terrorist attacks in 2016-2017.[63] As a result of the influx of terror attacks, many European countries, like Germany, have taken it upon themselves to start fighting terrorism online.[64] Under the new EU regulation, European nations have resorted to a mainly content-based social media regulation.[65] This new legislation takes into account social media's integral part with regards to terrorist recruitment

---

59. Parker & Sitter, *supra* note 45, at 211.

60. 18 U.S.C. § 2331 (2019).

61. *Id.*

62. *Id.*

63. Robin Simcox, *After a Lull, Islamist Terrorism in Europe Returns With a Vengeance*, HERITAGE FOUND. (Oct. 10, 2019), (https://www.heritage.org/terrorism/commentary/after-lull-islamist-terrorism-europe-returns-vengeance [https://perma.cc/PWZ3-NFU5].

64. *See, e.g.*, *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG) – Basic Information*, FED. MIN. JUST. & CONSUMER PROT., https://www.bmjv.de/DE/Startseite/Startseite_node.html [https://perma.cc/PKD9-TWUM] [hereinafter *Act to Improve Enforcement of the Law in Social Networks*].

65. *See, e.g.*, Joris van Hoboken et al., *The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications*, TRANSATLANTIC WORKING GROUP (May 3, 2019), https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf [https://perma.cc/GXN6-3YT3].

and propaganda.[66] The regulation was first proposed in September 2018.[67] The main reason for the push towards this legislation was the change in tactics and influx in self-radicalization.[68] The British Security Commissioner, Julian King, stated in Brussels, that "there had been a shift in the nature of terror attacks, with people being increasingly radicalised and then receiving instructions online . . . digital material played a part in every attack in Europ[e] in the past 18 months."[69] Another senior advisor proponent of the new law, Lucinda Creighton, of the Counter Extremism Project, a group that helped outline the regulation, says "whether it was the Nice attacks, whether it was the Bataclan attack in Paris, whether it's Manchester, . . . they have all had a direct link to the online extremist content."[70]

Before the proposal of this piece of legislation, the European Union had put in place a system of "voluntary frameworks and partnerships including the EU Internet Forum which was launched in December 2015 under the European Agenda on Security."[71] The EU Internet Forum focused on voluntary cooperation between online service providers and national governments. This voluntary partnership focused on limiting the amount of terrorist content online and "empower[ing] civil society to increase the volume of effective, alternative narratives online."[72] The EU Internet Forum has worked in most respects. It has increased cooperation between those in the tech industry and national governments; it has improved the response time of the industry to national governments and to Europol's Internet Referral Unit; it has increased the proactive measures to detect terrorist content; and lastly, it has increased the transparency of such efforts.[73]

While the voluntary system of the EU Internet Forum has worked in some regards, its voluntary nature has proven limitations. First, the European Commission, in its proposal for the new EU regulation, outlines that the voluntary nature of the Forum has meant that not all hosting service providers have participated.[74] Secondly, the Forum does not work at a pace nor a scale that will provide for adequate redress of the terrorist presence on social media.[75]

---

66. Porter, *supra* note 26.

67. *Id.*

68. Daniel Boffey, *Remove Terror Content or be Fined Millions, EU Tells Social Media Firms*, THE GUARDIAN (Sept. 13, 2018), https://www.theguardian.com/media/2018/sep/13/social-media-firms-could-face-huge-fines-over-terrorist-content [https://perma.cc/RT9H-JCPT].

69. *Id.*

70. Porter, *supra* note 26.

71. *Commission Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*, at 1, COM (2018) 640 final (Dec. 12, 2018).

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.* at 2.

The European Union is not alone in its call for a more enhanced action plan.[76] Germany has implemented the Network Enforcement Act, commonly known as NetzDG.[77] Germany's law targets hate crimes, terrorist content, fake news, malicious gossip, defamation, incitement to hatred, and other unlawful content.[78] In 2017, the European Council called on the industry to make changes to their existing terrorist content monitoring and response systems; "to develop new technology and tools to improve the automatic detection and removal of content that incites terrorist acts."[79] Europol called the European Terrorist Content Regulation "a coherent and coordinated European prevention approach."[80]

The European Council, Commission, and Parliament have all taken steps towards drafting their version of the Terrorist Content Regulation. Currently, the proposed regulation is being drafted to its final version.[81] However, on April 17, 2019, after a plenary session, the European Union Parliament voted to adopt amendments to the original December 2018 proposal by the Commission.[82] With a vast majority of votes in favor of the adoption, many concerns of the original proposal were quelled.[83]

The proposed EU legislation "set[s] a minimum set of duties of care on hosting service providers," without regard to their main place of origin."[84] The European Union places much of the burden on hosting service providers.[85] A "hosting service provider" is defined, under the Terrorist Content Regulation, as a provider of whose services "consists [of] the storage and processing of online information provided by and at the request of the" user and make the information

---

76. *Id.*

77. *Act to Improve Enforcement of the Law in Social Networks*, *supra* note 68.

78. *Id.*

79. *Commission Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*, at 2, COM (2018) 640 final (Dec. 12, 2018).

80. *Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda*, EUROPOL (July 1, 2015).

81. Daphne Keller, *The CJEU's New Filtering Case, the Terrorist Content Regulation, and the Future of Filtering Mandates in the EU*, CTR. INTERNET & SOC'Y (Dec. 2, 2019), http://cyberlaw.stanford.edu/blog/2019/12/cjeu%E2%80%99s-new-filtering-case-terrorist-content-regulation-and-future-filtering-mandates-eu [https://perma.cc/4X67-T2AG].

82. Vinenzo Tiani, *European Parliament Vote Addresses Core CDT Concerns with the Proposed Regulation on Terrorist Content Online*, CTR. DEMOCRACY & TECH. (Apr. 19, 2019), https://cdt.org/insights/european-parliament-vote-addresses-core-cdt-concerns-with-the-proposed-regulation-on-terrorist-content-online/ [https://perma.cc/L9GB-ZM2Y]; *see* Colin Lecher, *Aggressive New Terrorist Content Regulation Passes EU Vote*, THE VERGE (Apr. 17, 2019), https://www.theverge.com/2019/4/17/18412278/eu-terrorist-content-law-parliament-takedown [https://perma.cc/62MD-YGMA]; s*ee also* EUR. PARL. DOC. (COM 0640) (2019).

83. Tiani, *supra* note 82; Lecher, *supra* note 82.

84. *Commission Proposal*, *supra* note 26, at 2, 23.

85. *Id.* at 22-3.

provided available to third parties.[86] In their amendment, the EU Parliament reiterates that this description only applies to "services provided to the public at the application layer," and does not include cloud infrastructure or electronic communications services defined in Directive (EU) 2018/1972.[87]

The key part of this legislation is the definition of terrorist content. Before the April 2019 plenary session, there were three policy options considered "besides the baseline scenario" for how "terrorist content" would be defined.[88] The key differences between each of these policies were between "the scope of the definition of terrorist content, the level of harmonisation of referrals, the scope of proactive measures, co-ordination obligations on Member States, as well as data preservation requirements."[89] The first option was a more narrow definition, and would have limited the scope to only content that "directly incite[s] commit[ment] of a terrorist act."[90] The hosting service provider would have the option to take proactive measures to address the risk. The second option, as well as the third option, was focused on the content covered by option one and content concerning recruitment. However, the second option was requiring the creation of automatic tools to prevent re-posting of the content. The third option was requiring hosting service providers to detect new content.[91]

There were many critics of this proposed regulation who were concerned with how broad the definition in the December 2018 proposal was.[92] The original definition included any acts that incited, glorified, or advocated for the commission of terrorist offenses and any acts that promoted terrorist activities or instructed on how to commit a terrorist offense.[93] In the adopted version, the EU Parliament narrowed the definition and explicitly excluded any materials used for "educational, journalistic or research purposes or for awareness-raising purposes against terrorist activity."[94] Terrorist content is now defined as:

> (a) inciting the commission of one of the offences listed in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such conduct, directly or indirectly, such as the glorification of terrorist acts, advocates the commission of terrorist offences whereby causing a danger that one or more such offences may be committed intentionally;
> (b) soliciting another person or group of persons to commit or contribute to the commission of one of the offences listed in points (a) to (i) of

---

86. *Report on Commission Proposal*, *supra* note 26, at 35; *see also* Commission Proposal, *supra* note 26, at 22.

87. *Report on Commission Proposal*, *supra* note 26, at 36; *see also* Directive (EU) 2018/1972.

88. *Commission Proposal*, *supra* note 26, at 6.

89. *Id.* at 7.

90. *Id.*

91. *Id.*

92. Tiani, *supra* note 82.

93. *Commission Proposal*, *supra* note 26, at 23-4; *see also* Tiani, *supra* note 82.

94. *Report on Commission Proposal*, *supra* note 26, at 61.

> Article 3(1) of Directive (EU) 2017/541, thereby causing a danger that one or more such offences may be committed intentionally;
> (c) soliciting another person or group of persons to participate in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way within the meaning of Article 4 of Directive (EU) 2017/541, thereby causing a danger that one or more such offences may be committed intentionally;
> (d) providing instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences listed in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.[95]

A "competent authority" in the Member States will use this definition to notify hosting service providers of potential terrorist content on their platforms.[96] These authorities and the Member States will work through "a framework of voluntary cooperation."[97] The competent authority will be decided by the Member State, allowing them to designate an independent administrative, judicial, or law enforcement authority.[98] It is defined as "single designated judicial authority or functionally independent administrative authority in the Member State."[99] The regulation requires Member States to ensure that the competent national authority is capable of detecting and altering hosting service providers of the offending content.[100] Once a hosting service provider is informed of terrorist content, they are required to remove it within one hour.[101] The "systematic and persistent" failure to take down the offending content could lead to fines of up to four percent of the hosting service provider's annual global revenue.[102] A social media company like Facebook, which has an annual revenue of $17 billion, could face fines of up to $680 million.[103] However, the final decision to remove the content would be "a voluntary decision by the hosting service provider.[104] The removal orders "would be subject to judicial redress," which would prevent content from

---

95. *Id*. at 37-38; *see also* Article 3(1) of Directive (EU) 2017/541. *See generally* Commission Proposal, *supra* note 26, at 23-24.

96. *Commission Proposal*, *supra* note 26, at 3, 24; *see also* Alexander Pirang, *The EU Terrorist Content Regulation is Unfinished Business for the European Parliament*, GLOB. PUB. POL'Y INST. (May 23, 2019), https://www.gppi.net/2019/05/23/unfinished-business-for-the-european-parliament-the-eu-terrorist-content-regulation [https://perma.cc/8K8R-5TZ8].

97. *Report on Commission Proposal*, *supra* note 26, at 9.

98. *Id.* at 17; Porter, *supra* note 26; Tiani, *supra* note 82.

99. *Report on Commission Proposal*, *supra* note 26, at 40.

100. *Commission Proposal*, *supra* note 26, at 4.

101. *Report on Commission Proposal*, *supra* note 26, at 43-44.

102. *Id*. at 62.

103. Porter, *supra* note 26.

104. *Commission Proposal*, *supra* note 26, at 5.

being removed that was not terrorist content.[105]

The regulation, in addition to the removal procedures, would also create a network by which Member States work with each other and law enforcement.[106] Member States would be obligated to inform and work with other States regarding removals and referrals.[107] The regulation may require Member States to inform law enforcement about the procedures they took when they identified terrorist content when it poses a safety risk.[108] Lastly, hosting service providers would be required to preserve the content that they found and removed.[109] However, this does not allow for a general obligation to monitor or search for information or circumstances that indicate illegal activity.[110] This would help "safeguard against erroneous removal and ensures potential evidence is not lost for the purpose of the prevention, detection, investigation, and prosecution of terrorist offences."[111]

Advocates praise the regulation for its"common-sense proposals," which will help stop the dissemination of terrorist content online.[112] However, for as many advocates as this bill has, it has double the number of critics.[113] Their main concern is how this regulation will affect the fundamental rights of EU citizens.[114] In a letter to the European parliament, the European Digital Rights or the EDRi stressed the importance of "fundamental pillars of European Union law" and "*any* measure implemented to fight terrorism must be appropriate, necessary and proportionate."[115] Anything less than these requirements would be a sacrifice of

---

105. *Report on Commission Proposal*, *supra* note 26, at 44; *see also Commission Proposal*, *supra* note 26, at 7.

106. *Report on Commission Proposal*, *supra* note 26, at 61.

107. *See Commission Proposal*, *supra* note 26, at 4.

108. *Commission Proposal*, *supra* note 26, at 4.

109. EUR. PARL. DOC. (COM 0640) 90-93 (2019); *see also Commission Proposal*, *supra* note 30, at 4.

110. EUR. PARL. DOC. (COM 0640) 12 (2019).

111. *Commission Proposal*, *supra* note 26, at 4.

112. Porter, *supra* note 26.

113. *See, e.g.*, *Press Release: EU Parliament Deletes the Worst Threats to Freedom of Expression Proposed in the Expression Proposed in the Terrorist Content Regulation*, EUR. DIG. RTS. (Feb. 19, 2020), https://edri.org/eu-parliament-deletes-worst-threats-to-freedom-of-expression-terrorist-content-regulation/ [https://perma.cc/MG8U-4SLM] [hereinafter *Press Release*]; Diego Naranjo, *CULT: Fundamental Rights Missing in the Terrorist Content Regulation*, EUR. DIG. RTS. (Jan. 21, 2019), https://edri.org/cult-fundamental-rights-missing-in-the-terrorist-content-regulation/ [https://perma.cc/N2DP-WHRP]; Porter*, supra* note 26.

114. Porter*, supra* note 26; *Press Release*, *supra* note 113.

115. *Recommendations for the European Parliament's Draft Report on the Regulation on preventing the Dissemination of Terrorist Content Online*, EUR. DIG. RTS. 2 (Dec. 2018), https://edri.org/files/counterterrorism/20190108_EDRipositionpaper_TERREG.pdf [https://perma.cc/6W5Q-RGF2] [hereinafter *Recommendations for the European Parliament's Draft Report on the Regulation*] (emphasis added).

fundamental rights.[116] First, the definition of "terrorist content" is too broad.[117] The Transatlantic Working Group stated that with the inherent difficulty of defining terrorism, the proposed regulation should "strictly follow established rule of law and freedom of expression requirements."[118] They also stated that there needs to be an intent requirement in the proposal's definition of terrorist content.[119] Many fear that the broad nature of the definition could allow for overt censorship on social media platforms.[120] Opponents fear the legislation could end up like YouTube's Content ID system, which has been heavily criticized. The Content ID system "allows copyright owners to file takedowns on videos that use their material," however, sometimes, videos are taken down after being posted by the copyright owners.[121] In other words, there is no guarantee that software will be 100% correct with every video or post that is removed from social media. Technology has its limitations, and this has human rights activists worried.[122] The EDRi, cited the UN Special Rapporteur, saying that the proposal should focus solely on *illegal* terrorist content.[123] For example, many NGOs reporting on the Syrian war were "undermined by blocking of legal content by internet companies, which significantly affected the documentation of acts of violence against civilians."[124] Google took down over 100,00 videos, between 2012 and 2018, concerning the Syrian conflict. This led to "vital evidence of what took place" being destroyed and lost.[125]

Additionally, another concern for opponents of the proposal is the strict one-hour takedown policy.[126] They state that it is too rigid and places a high burden on small Internet companies.[127] A flexible removal time "would signal similar urgency, while better respecting established freedom of expression and due process rights."[128] It would also afford Internet companies time to raise legitimate issues or objections to the removal before removing it.[129] According to Lucinda Creighton of the Counter Extremism Project, as mentioned above, this tight time limit is essential to stop it from spreading. She states that research has proven that if the "content is left up for more than one hour, 'it's viewership increases.'"[130]

---

116. *Id.*

117. *See id.*; Hoboken et al., *supra* note 65, at 2.

118. Hoboken et al., *supra* note 65, at 2.

119. *Id*. at 4.

120. *Id*. at 2.

121. Porter*, supra* note 26.

122. *Press Release*, *supra* note 113; *see also* Pirang, *supra* note 96.

123. *Recommendations for the European Parliament's Draft Report on the Regulation*, *supra* note 125, at 6.

124. *Id.* at 5.

125. Porter, *supra* note 26.

126. Hoboken et al., *supra* note 65, at 2.

127. *Id.*; Pirang, *supra* note 96.

128. Hoboken et al., *supra* note 65, at 2; Pirang, *supra* note 96.

129. Pirang, *supra* note 96.

130. Porter, *supra* note 26.

Although this research was focused on YouTube, the time limit would apply to all social media platforms.[131]

Lastly, opponents of the proposal believe that the current voluntary system under the EU Internet Forum is enough to stop the dissemination of terrorist content online. They claim that the voluntary system has removed a majority of terrorist content from major social media platforms, stating that users need "to go out of their way to find the [terrorist] content on a smaller site." Jens-Henrik Jeppesen, of the Center for Democracy and Technology ("CDT"), is one of the biggest opponents to the regulation, states "it is disproportionate to have new legislation to see if you can sanitize the remaining 5 percent of available platforms." Lucinda Creighton, as mentioned above, believes that this new regulation will hold every social media company to the same standards and help promote transparency. Currently, social media platforms have their own ways of monitoring and removing offensive content; the regulation will help streamline and allow the public to know how platforms are monitored. Creighton states that these proposals will help benefit the Member States and law enforcement due to the obligation of sharing information. However, "it has the potential to lock out non-governmental bodies like the Syrian Archives if governments don't give them access to the extremist content." Public access to this content, according to Creighton, is not enough to justify their (NGOs and the public) access to the removed content.[132] The proposed Terrorist Content Regulation has yet to be finalized.

II. THE AMERICAN APPROACH

Unlike the European Union and its Member States, the United States has not taken such broad steps to create government regulation for terrorist online propaganda. It is a contentious issue that has captured the minds of many lawmakers and everyday Americans. The increase in terror attacks that have been instigated by social media has only fueled the country's debate on government regulation of social media. The United States has the Constitutional guarantee of free speech to contend with. In recent years, individuals and lawmakers have attempted to stop terrorist dissemination of propaganda by holding tech giants liable. This circumvents the problem and ongoing debate of outright government regulation and monitoring of the internet by looking to tech companies as the gatekeepers. The European Union, by contrast, has used government regulation to create a list of unacceptable terms and phrases that should be used by tech companies to monitor their respective platforms. This indirect regulation on social media content has had some success; however, there is a roadblock to this way of regulating: Section 230 of the Communications Decency Act. As this note will explore in the coming sections, Section 230 has created the ultimate trump card for tech companies.

---

131. *Id.*

132. *Id.*

A. Material Support of Designated Terrorist Organizations: 18 U.S.C. 2339(b)

In response to the growing threat of international terrorism in the 1990s, following the end of the Cold War, the United States passed laws targeting the material support of terrorists. Section 2339(b) was passed as a part of the 1996 Antiterrorism and Effective Death Penalty Act (AEDPA). The new Section reflected Congress' intent to recognize "the fungibility of financial resources and other types of material support." Unlike 18 U.S.C. § 2339(A), which prohibits providing material support to anyone who may commit an act in a "terrorism context," Section 2339(b) focuses on providing material support to foreign terrorist organizations.[133] 18 U.S.C. § 2339(b) states:

(1) whoever
(2) knowingly
(3)(a) attempts to provide,
    (b) conspires to provide, or
    (c) provides
(4) material support or resources
(5) to a foreign terrorist organization
(6) knowing that the organization
    (a) has been designated a foreign terrorist organization, or
    (b) engages, or has engaged, in "terrorism" or "terrorist activity."[134]

Section 2339(b) rests partly on groups that have been designated as foreign terrorist organizations (FTOs).[135] The designation of groups as foreign terrorist organizations is determined by the Secretary of State.[136] The Secretary designates groups when they have found that the organization is (1) a foreign organization, (2) that engages in terrorist activity (defined by 8 U.S.C. 1189(a)(3)(B)) or terrorism (defined in 22 U.S.C. 2656f(d)(2)) or has the capability and intent to carry out terrorism or terrorist activity, (3) the activities and actions of the organization threaten United States national security or Americans.[137] Upon being designated as an FTO, the Secretary will publish the designation in the Federal Register.[138] A group that has been designated as a foreign terrorist organization can request judicial review of the designation.[139] The petition for judicial review can happen no later than 30 days after the publication of the Secretary's findings in the Federal Register.[140]

---

133. Charles Doyle, *Terrorist Material Support: An Overview of 18 U.S.C. §2339A and §2339B*, CONG. RSCH. SERV. 1 (Dec. 8, 2016).

134. 18 U.S.C. § 2339(b)(a)(1).

135. *Id.*

136. 8 U.S.C. § 1189(a)(1).

137. *Id.*

138. *Id.* § 1189(a)(2)(ii).

139. *Id.* § 1189(a)(4).

140. *Id.* § 1189(c)(1).

1. The Mens Rea: Knowingly Providing Support to an FTO

Section 2339(b) outlines that anyone who *knowingly* attempts or does provide support to a designated foreign terrorist organization or a group that engages in terrorist activity or terrorism shall be found liable either criminally or civilly.[141] The required knowledge element if Section 2339(b) has been challenged in courts. There are two knowledge elements in the statute. The government has the burden to prove that the defendant knew or was aware that the group or organization they were providing resources to was an FTO or a group that partook in terrorism or terrorist activity. The second knowledge element was that the defendant knowingly or was at least aware that they were providing that organization with resources or supplies.[142] Aside from those knowledge requirements, Congress did not require the defendant to have a mens rea of specific intent.[143] The government, then, does not need to prove that the defendant's goal was "to further a foreign terrorist organization's illegal activities."[144]

In *Crosby v. Twitter*, the plaintiffs were the victims or families of those who were killed in the Pulse Night Club Shooting in Orlando, Florida, on June 12, 2016. The plaintiffs did not bring suits against Omar Mateen, the perpetrator. They brought claims under the ATA against Facebook, Twitter, and Google. They alleged that the tech giants allowed ISIS to use "social media platforms to post propaganda and 'virtually recruit' Americans to commit terrorist attacks."[145] This "virtual recruiting" had worked on Mateen, "the FBI determined that he was self-radicalized."[146] He never had contact with ISIS, directly; and he was radicalized by ISIS propaganda and jihadist videos. However, his radicalization occurred "over a period of several years and [Mateen] decided only recently before the attack to embrace [ISIS]."[147] The plaintiffs allege that because he was radicalized by terrorist content that was on the defendant's social media platforms, that they violated 18 U.S.C. § 2339(b).[148]

The plaintiffs, while in District Court, contended that the defendants supplied ISIS and, thus Mateen, with material support in violation of Section 2339(b). On appeal, the plaintiffs dropped this material support claim. The material support was in the form of ISIS having accounts of the defendant's social media platforms and the fact that Mateen was radicalized on those platforms. The plaintiff's district court allegations and eventual dismissal prove how difficult it is and how reluctant the court is to bring a Section 2339(b) claim. The court ruled that the

---

141. 18 U.S.C. § 2339(b)(a)(1).

142. Doyle, *supra* note 133, at 14.

143. Holder v. Humanitarian Law Project, 561 U.S. 1, 2709 (2010).

144. *Id*. at 2706.

145. Crosby v. Twitter, Inc., 921 F.3d 617, 619 (6th Cir. 2019).

146. *Id*. at 621.

147. *Id*.

148. *Id*.

connection between the tech companies and the actions by Mateen was not tangible enough.[149]

In *Fields v. Twitter*, the plaintiffs sued Twitter under the Anti-Terrorism Act; and alleged that Twitter knowingly allowed ISIS members to have Twitter accounts, thus in violation of 18 U.S.C. § 2339(b).[150] The plaintiffs sought civil remedies under 18 U.S.C. § 2333, which provides remedies for United States nationals who have an injury to themselves, property or business because of an act of international terrorism.[151] If it can be proven under § 2339(b) that there was material support, "and that it also qualifies as an act of 'international terrorism' under 18 U.S.C. § 2331(1)," a plaintiff can then seek remedies for injuries if they occurred "'by reason of' the defendant's conduct" under 18 U.S.C. § 2333(a).[152]

In *Fields*, the widows and children of Lloyd "Carl" Fields Jr. and James Damon Creach, who were government contractors, filed a suit against Twitter.[153] Fields and Creach were killed in an attack for which ISIS claimed credit.[154] The plaintiffs "contend that '[s]ince 2010, Twitter has provided (and thus materially supported) ISIS with dozens of accounts on its social network,' and until recently did nothing while 'the number of ISIS accounts on Twitter grew at an astonishing rate.'"[155] The amount of pro-ISIS tweets and accounts are not new information for the public or the courts. During a hearing before the Subcommittee on National Security, then-representative Ron DeSantis stated:

> There are 90,000 pro-ISIS tweets on a daily basis. While others suggest that there may be as many as 200,000 such tweets. Accounts belonging to other foreign terrorist organizations . . . have a total of over 200,000 followers and are thriving . . . ISIS's use of platforms like Twitter is highly effective.[156]

The *Fields* case shows the number of hurdles a plaintiff faces in proving an ATA claim against a technology company. The Court focused most of its attention on the plaintiff's Section 2333 claim for civil remedies and found that the plaintiffs could not recover because they could not satisfy the "by reason of" requirement to recover under Section 2333.

The *Fields* and *Crosby* cases show the difficulty of proving the mens rea requirement of Section 2339(b). Aside from proving the connections between a social media company and an FTO, it is hard to be certain that the user is, in fact, an FTO. The overall anonymity of the internet, as discussed above, is a central theme on social media and a key part of why terrorists use the internet. It is not unusual for an FTO to use false identities while on social media: "[I]nvestigators

---

149. Crosby v. Twitter, Inc., 303 F. Supp. 3d 564, 576 (E.D. Mich. R. 2018).

150. Fields v. Twitter, Inc., 881 F.3d 739, 742 (9th Cir. 2017).

151. 18 U.S.C. § 2333(a).

152. Crosby v. Twitter, Inc., 921 F.3d 617, 622 (6th Cir. 2019).

153. *Fields*, 881 F.3d at 741.

154. *Id.* at 41-42.

155. *Id.* at 42.

156. *See, e.g.*, *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 16, at 1.

have revealed how terrorist groups systematically conceal their activities behind charitable, social, and political fronts."[157] This complicates the court's job in deciding if the defendant had the requisite mens rea. It would be too much to ask that each social media company be required to vet and verify that each user is whom they say they are.

2. What is Material Support?

The term "material support" has been altered periodically since 2339(b)'s enactment.[158] Currently, material support includes anything from training and expert advice to weapons and explosives to communication and financial services. However, material support does not include religious materials or medical supplies.[159] In 2010, the Supreme Court ruled that it is not unconstitutional to criminally prohibit those who "engag[e] in coordinated teaching and advocacy furthering" a designated terrorist organization, regardless of humanitarian objectives.[160] The ruling in *Holder v. Humanitarian Law Project* further expanded the 1990s era anti-material support statute's definition of material support to now include humanitarian aid and, most importantly, any action that is in "service to" an FTO.[161] The Court considered the words in "service to" to mean a connection between the service given and the FTO.[162] This includes any "advocacy performed in coordination with, or at the direction of, a foreign terrorist organization."[163] However, this did not prohibit individuals from simply advocating for the FTOS, nor did it prohibit them from claiming affinity with the FTOS or adopting their political stances.[164] The Court rested their case on the fact that even:

> Material support meant to 'promot[e] peaceable, lawful conduct,'. . . can further terrorism by foreign groups in multiple ways . . . Such support frees up other resources within the organization that may be put to violent ends. It also importantly helps lend legitimacy to foreign terrorist groups--legitimacy that makes it easier for those groups to persist, to recruit members, and to raise funds--all of which facilitate more terrorist attacks.[165]

The plaintiffs, namely the Humanitarian Law Project, in *Holder*, sought to

---

157. Holder v. Humanitarian Law Project, 561 U.S. 1, 30 (2010).

158. *Id.* at 8.

159. Charles Doyle, *supra* note 133, at 15.

160. *Humanitarian Law Project*, 561 U.S. at 41.

161. *Id.* at 24.

162. *Id*.

163. *Id*.

164. Alexander Tsesis, *Social Media Accountability for Terrorist Propaganda*, 86 FORDHAM L. REV. 607, 615 (Oct. 4, 2017) [hereinafter *Social Media Accountability for Terrorist Propaganda*]; Humanitarian Law Project, 561 U.S. at 26.

165. *Humanitarian Law Project*, 561 U.S. at 30.

provide political and humanitarian support to two international organizations: the Partiya Karkeran Kurdistan (PKK) and the Liberation Tigers of Tamil Eelam (LTTE).[166] The claim brought by the plaintiffs alleged that it is unconstitutional for Section 2339(b) to prohibit "four types of material support –'training,' 'expert advice or assistance,' 'service,' and 'personnel.'"[167] The Humanitarian Law Project wished to teach the "PKK members [how] to use international law to resolve disputes peacefully; teaching PKK members to petition the United Nations and other representative bodies for relief; and engaging in political advocacy on behalf of Kurds."[168] Both the PKK and the LTTE have been designated as foreign terrorist organizations by the United States government.[169]

Plaintiffs asserted that the prohibition violated their Fifth Amendment Due Process rights and their First Amendment right to free speech and expression.[170] They claimed that the prohibition on providing training violated the Fifth Amendments Due Process Clause on the basis that it was unconstitutionally vague and that it might extend into lawful advocating and support.[171] The Plaintiffs also had a First Amendment claim based on the fact that their right to free speech and freedom of association had been violated. Ultimately, the Supreme Court determined that the provision was not unconstitutional.[172] The Chief Justice stated that "a plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others."[173]

In addressing the plaintiff's First Amendment claims, the Court concluded that "Congress may outlaw material support to a terrorist organization in the form of speech of the type at issue without offending the First Amendment."[174] The Chief Justice quickly disposed of their freedom of association claims, stating that the statute prohibited conduct and not membership.[175] In its findings, the Court showed that the government's compelling interest to stop terrorism was enough to prohibit the advocacy and humanitarian support of foreign terrorist organizations.[176]

The Court in *Humanitarian Law Project* deemed that to be material support under Section 2339(b), the defendant must have acted in coordination with an FTO. The Court, however, left the question open as to how much coordination

---

166. *Id.* at 2.

167. *Id.*

168. *Id.*

169. *Id.*

170. *Id.*

171. Doyle, *supra* note 133, at 16.

172. *Id.*

173. *Humanitarian Law Project*, 561 U.S. at 19-20 (quoting Hoffman Estates v. Flipside, 255 U.S. 489, 495 (1982)).

174. Doyle, *supra* note 153, at 16.

175. *Humanitarian Law Project*, 561 U.S. at 39.

176. Doyle, *supra* note 152, at 16.

is needed to be deemed material support.[177] If it is found that the bar for coordination is low, then it is possible for social media providers to be considered to be materially supporting FTOs. In 2013, the First Circuit provided some guidance on this contention.[178] In *United States v. Mehanna*, an American living in Massachusetts was charged with numerous terrorist-related offenses, including one charge concerning the translation of Arab-language materials and posting them on a website that had Al Qaeda and jihadist sympathies.[179]

Prior to translating documents, Mehanna had spent time in Yemen, in an attempt to join Al Qaeda.[180] The translated materials were related to terrorism in varying degrees.[181] Some of the materials were "al Qaeda–generated media and materials supportive of al-Qaeda and/or jihad, such as instructing readers to 'ask God for martyrdom' and to 'Go for Jihad Yourself,' to more innocuous writings loosely tethered to the jihad movement, such as maintaining physical fitness."[182] Mehanna had argued that his translations should be considered independent advocacy under *Humanitarian Law Project*.[183] This would cause Mehanna's translations to be protected under the First Amendment.[184] He argued that the jury had not been properly instructed on what the meaning of "coordination" was under *Humanitarian Law Project.*[185] The First Circuit, however, affirmed the conviction of Mehanna, thus raising interesting questions as to speech and material support of FTOs.[186] The court stated that the jury instructions of the trial judge: "[i]ndividuals who act entirely independently of the 'FTO' to advance its goals or objectives shall not be considered to be working under the FTO's direction," was an accurate definition of coordination.[187] Mehanna contended that for there to be a violation, there needed to be a direct link between the FTO and a defendant.[188] The Court noted that there is nothing in Section 2339(b) or in the Supreme Court's ruling in *Humanitarian Law Project* regarding how much coordination is needed to be considered a direct link.[189] The First Circuit's ruling failed to definitively answer questions about coordination by affirming the

177. *Humanitarian Law Project*, 561 U.S. at 24.

178. United States v. Mehanna, 735 F.3d 32 (1st Cir. 2013).

179. *Id.* at 41.

180. *Id.*

181. Michal Buchhandler-Raphael, *Overcriminalizing Speech*, 36 CARDOZO L. REV. 1667, 1669 (2015).

182. *Id.* (citing Muhammad bin Ahmad as-Salim, *39 Ways to Serve and Participate in Jihad*, AT-TIBYĀN PUBL.).

183. *Mehanna*, 735 F.3d at 47.

184. *Id.*

185. *Id.*

186. *See, e.g.*, Buchhandler-Raphael, s*upra* note 181, at 1669.; Kathleen Ann Ruane, *How Broad a Shield? A Brief Overview of Section 230 of the Communications Decency Act*, CONG. RSCH. SERV. 3, 17 (Feb. 21, 2018).

187. *Mehanna*, 735 F.3d at 48-49.

188. *Id.* at 50.

189. *Id.*

conviction on the grounds that Mehanna's time in Yemen was enough to establish guilt, regardless of whether or not his translation activities were protected by the First Amendment.[190] The confusion surrounding the coordination requirement continues after the Supreme Court denied certiorari for Mehanna.[191] The future of material support claims used in connection with social media posts is yet to be seen.

B. Section 230 of the Communications Decency Act

The Material Support statute stated above is being looked at as a way to stop the dissemination of terrorist propaganda online. However, in 1996, Congress provided tech companies with the ultimate "get out of jail free card:" the Communications Decency Act (CDA).[192] The goal of the Act was to provide "immunity from liability for providers and users of interactive computer service[s] who publish information provided by" their users.[193] The Act lays out that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[194] Congress effectively provided companies who are interactive computer service providers immunity from lawsuits arising out of opinions and materials circulated by them but posted by third-party users.[195] The CDA "was passed to enhance service providers' ability to delete or otherwise monitor content without them [the companies] becoming publishers."[196] This kind of legal protection is wholly unique to the United States. It reflects the valued idea of the "marketplace of ideas."[197] Since Justice Oliver Wendell Holmes' dissent in *Abrams v. United States*, the marketplace of ideas has been used as the rationale behind the First Amendment.[198] The marketplace of ideas is the concept that "the best test for truth is the power of the thought to get itself accepted in the competition of the market."[199] This concept "has been influential in the Court's Internet-related jurisprudence," and thus the Court's interpretation of the

---

190. *See* Emily Goldberg Knox, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 Hastings L.J. 295, 314-15 (Dec. 2014); Ruane, *supra* note 186, at 17.

191. *See* Mehanna v. United States, 574 U.S. 814 (2014)

192. *What is Section 230 of the Communication Decency Act (CDA)?*, MINC L., https://www.minclaw.com/legal-resource-center/what-is-section-230-of-the-communication-decency-act-cda/ [https://perma.cc/K6ST-UFK4][hereinafter What is Section 230].

193. *Id.*

194. *CDA 230: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUND, https://www.eff.org/issues/cda230 [https://perma.cc/R55B-8NLN].

195. Klayman v. Zuckerberg, 910 F. Supp. 2d. 314, 318 (D.C. Cir. 2012).

196. *What is Section 230*, *supra* note 192.

197. Steven Beale, *Online Terrorist Speech, Direct Government Regulation, and the Communications Decency Act*, 16 DUKE L. & TECH. REV. 333, 335-36 (2018).

198. *Id.*

199. *Id.*

Communications Decency Act.[200] The Act itself notes that it was inspired by the concept of the marketplace of ideas.[201] Additionally, the CDA provides Internet providers with a "safe haven" for their platforms.[202]

When Congress passed Section 230, they could not have known how broad and widespread the law would become. The Act has been expanded by the courts, which "have extended this safe harbor far beyond what the provision's words, context, and purpose support."[203] The Fourth Circuit held in *Zeran v. America Online* that it was Congress' intention for Section 230 to provide broad immunity.[204] Lawsuits that arose from a service provider exercising their "traditional editorial functions" will be dismissed.[205] "Traditional editorial functions" were defined by the court in *Zeran* as "decisions [on] 'whether to publish, withdraw, postpone, or alter content.'"[206] The rationale was that internet service providers, when liable for every message that passes through their platform "might choose to severely restrict the number and type of messages posted."[207] Congress, considering the effect this could have on the First Amendment and the influence of the marketplace of ideas, decided to make the Act broad. The Communications Decency Act "provides a significant additional protection to online speech that supplements the already very strong protections provided by the First Amendment and the Supreme Court's current jurisprudence."[208]

The liability shield provided by Section 230 is not all encompassing. Section 230(e) provides an exception to an interactive service provider's immunity from liability.[209] The shield does not apply to intellectual property, federal criminal law, and the Electronic Communications Privacy Act of 1986.[210] However, in 2018 Congress created another statutory exception in the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, or commonly known as FOSTA.[211] With the passage of FOSTA, tech companies and other companies designated as interactive service providers cannot use Section 230 as a defense.[212] FOSTA removes immunity from interactive service providers who "unlawfully

---

200. *Id.* at 336.

201. *Id.*

202. *CDA 230: The Most Important Law Protecting Internet Speech*, *supra* note 194.

203. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401, 403 (2017) (citing Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 116 (2009)).

204. *What is Section 230*, *supra* note 192.

205. Klayman v. Zuckerberg, 910 F. Supp. 2d. 314, 319 (D.C. Cir. 2012).

206. Zeran v. America Online, Inc., 129 F.2d 327, 330 (4th Cir. 1997).

207. *What is Section 230*, *supra* note 192.

208. Beale, *supra* note 197, at 338.

209. Ruane, *supra* note 186, at 2.

210. Valerie C. Brannon, *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*, CONG. RSCH. SERV. 1, 4 (June 6, 2019).

211. *Id.*

212. *Id.*

promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[213] The premise for its enactment is that the Communications Decency Act, according to Congress, was not to provide legal protection to users and interactive service providers that "facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[214] FOSTA provides that any tech companies that "knowingly, assist, support, or facilitate advertising activity that violates federal sex-trafficking law, specifically [18 U.S.C. §]1592" will not be given immunity under the CDA.[215] Prior to FOSTA, tech companies were liable under 18 U.S.C. § 1592 if they knowingly profited or benefited off of outlawed ads.[216]

There have been mixed responses to the enactment of this statutory exception. Many have applauded Congress for taking an affirmative step towards minimizing and punishing those that facilitate and promote ads or websites that help human traffickers; however, there is an equal amount of those that oppose the Act. There have been questions regarding the First Amendment and whether or not the Act violates it. Professor Alexandra Levy of the Notre Dame Law School "argues that the Act does not overcome the strict scrutiny test – a key requirement for content-based speech restrictions – because [the Act] is not narrowly tailored."[217]

The Communications Decency Act rests on a three-prong test. This test is used to evaluate whether immunity will be granted to the computer company. The first prong "is the defendant must be a provider or user of an interactive computer service."[218] An "interactive computer service" has been defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[219] The second is that the defendant must be seen as the publisher or speaker of the content at issue. Courts have construed the term "publisher" to refer "to one who 'review[s], edit[s], and decide[s] whether to publish *or to withdraw from* publication third-party

---

213. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, 18 U.S.C. §§ 1591, 1595, 47 U.S.C. 230.

214. *Id.*

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

216. *Id.*

217. Zeynep Ulku Kahveci, *Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA): Senate Passes Bill Making Online Platforms Liable for Third-Party Content Enabling Illegal Sex-Trafficking*, HARVARD J.L. & TECH. (Apr. 3, 2018), https://jolt.law.harvard.edu/digest/allow-states-and-victims-to-fight-online-sex-trafficking-act-fosta-senate-passes-bill-making-online-platforms-liable-for-third-party-content-enabling-illegal-sex-trafficking [https://perma.cc/RD77-WPNB].

218. *What is Section 230*, *supra* note 192.

219. 47 U.S.C. § 230 (f)(2).

content.'"[220] Lastly, the content at issue must come from an information content provider that is not the defendant, e.g., a user. An "information content provider" is defined under § 230 as: "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[221]

Since its passage, Courts have been elaborating on the inner workings of Section 230. In 1997, the Ninth Circuit in *Fair Housing v. Roommates.com* ruled that an Internet content provider needed to be a "passive publisher of the content." In this case, the use of *Roommates'* "search mechanisms and email notifications meant that it was neither a passive pass-through of information provided by others nor merely a facilitator of expression," was not a passive provider of the content. The Fourth Circuit in 2009 distinguished *Roommates* in *Nemet Chevrolet, Ltd. V. Consumeraffairs.com, Inc*. The Court ruled that a website's "structure and design . . . was not sufficiently contributing to the content to transform *Consumeraffairs.com* into an information content provider." The more a content provider is involved in the creation of the content at issue, if it is illegal, the more likely it will not be afforded immunity under Section 230.[222]

The sheer breadth of the Communications Decency Act has given tech giants the ability to defeat any litigation brought against them. However, many have still filed lawsuits against major social media companies like Facebook and Twitter. These lawsuits have attempted to hold these companies "liable for deaths in terrorist attacks under the Anti-Terrorism Act," citing that these companies have provided material support to terrorist organizations by allowing them to have accounts.[223] Courts look to the Communications Decency Act for reasons of dismissing these Anti-Terrorism Act cases. However, in *Force v. Facebook*, the court stated that claims that are "plausibly pled [under the Anti-Terrorism Act] would escape" the coverage of Section 230.[224] The court in *Force* ruled that "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform."[225] In other words, failure to remove users involves a publishing activity that is protected under Section 230.

As opposed to *Fields v. Twitter*, reliance on the Anti-Terrorism Act for the basis of their claim, the plaintiff in *Klayman v. Zuckerberg* looks to negligence and assault-based claims. The Court, again, dismissed the complaint pursuant to the Communications Decency Act. The plaintiff, Larry Klayman, sued after finding a Facebook page titled "Third Palestinian Intifada."[226] He claimed that the

---

220. Klayman v. Zuckerberg, 910 F. Supp. 2d. 314, 319 (D.C Cir. 2012).

221. 47 U.S.C. § 230 (f)(3).

222. *What is Section 230*, *supra* note 192.

223. Beale, *supra* note 197, at 338.

224. Force v. Facebook, Inc., 304 F. Supp. 3d 315, 331 (D. N.Y. 2018).

225. Jeffrey D. Neuburger, *Facebook Shielded by CDA Immunity Against Federal Claims for Allowing Use of its Platform by Terrorists*, NAT'L L. REV. (Aug. 9, 2019), https://www.natlawreview.com/article/facebook-shielded-cda-immunity-against-federal-claims-allowing-use-its-platform [https://perma.cc/7JUJ-EP99].

226. Klayman v. Zuckerberg, 910 F. Supp. 2d. 314, 316 (D.C. Cir. 2012).

untimely manner in which it took Facebook to remove the page only further encouraged the Intifada. Once on the Facebook page, Klayman saw that the page called for the "uprising beginning on May 15, 2011, after Muslim prayers [were] completed, announcing, and threatening that 'Judgment Day will be brought upon us only once Muslims have killed all the Jews.'"[227] The Public Diplomacy Minister of Israel notified Facebook and asked that the page be taken down. Eventually, the page was removed; however, Facebook "refused for many days."[228] In furtherance of his assault claims, Klayman argued that Facebook "'marketed, used, and allowed [Facebook] to be used' to 'intentionally, violently and without just cause' assault the plaintiff.'"[229]

As to his negligence claim, Klayman argued that Facebook "owed [him] a duty of care, which they violated and breached by allowing and furthering the death threats by the Third Palestinian Intifada, and . . . refusing . . . to remove these postings."[230] The plaintiff asserted that Facebook's liability was found in the fact that they were publishers.[231] Finding Facebook a publisher, whether by "'using' the website to post certain content (i.e., publishing); 'allowing' certain content to be posted to the website (i.e., deciding whether to publish) or by 'refusing' . . . to remove these postings.'"[232] The plaintiff also argues that while Facebook is a publisher, its liability derives from the contractual and fiduciary duties it owed the plaintiff.[233]

In determining the liability of Facebook, the Court uses the three-prong test highlighted above. First, the Court looks at whether Facebook is an information content provider. Other courts have stated that the relevant question should be whether the defendant "functions[s] as an 'information content provider' for the portion of the statement or publication at issue."[234] This way, an entity would only be held responsible for the content they actually created. Using this narrower definition of when an entity is an information content provider "preserves the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[235] Klayman only accused Facebook of encouraging the Third Palestinian Intifada by not removing the page in a timely manner. The untimely manner in which Facebook acted to remove the page after being warned of the terrorist content. The plaintiff's argument fell apart when he did not rest his argument on the fact that Facebook was the "publisher or speaker of the third party's content." The court ultimately dismissed this complaint further showing the breadth of Section

227. *Id.*
228. *Id.*
229. *Id.* at 319.
230. *Id.*
231. *Id.*
232. *Id.*
233. *Id.* at 320.
234. *Id.*
235. *Id.* at 321.

230.[236]

III. MATERIAL SUPPORT STATUTE AND SOCIAL MEDIA: A CONSTITUTIONAL DILEMMA

The internet has become the perfect breeding ground for terrorist groups to spread propaganda, recruit new members, or inspire lone-wolf attacks.[237] Social media has become "the accelerant. It's the thing that turbocharges a poisonous and powerful message."[238] Countries around the world, including the European Union, have taken it upon themselves to help curb the effects of international terrorism within their borders through monitoring and regulating social media. The United States, as stated above, has not taken such determinative steps towards preventing terrorist propaganda on social media. Currently, most of the burden has fallen on social media companies to monitor their own platforms for terrorist content. While this can be argued to have assisted in the lessening of widespread terrorist content, it can also be seen as ineffective. The prevention of terrorist content online is complex. It is not a simple issue; it involves First Amendment issues and the issue of extraterritoriality. These issues are coupled with the fact that the internet is not a straightforward platform. Certain things need to be considered when promulgating a statute to fight online terrorist content, like a lack of attribution, and a high degree of anonymity, as mentioned above. Each of the laws that this Note mentioned could be used to alleviate some of these issues and concerns.

To start with, the material support statute: 18 U.S.C. § 2339(b), after all, many could feel that providing terrorists with a platform that effectively is a launching point for recruitment, and propaganda, is material support.[239] Tashfeen Malik, one of the perpetrators in the San Bernardino shooting, used Facebook to announce her allegiance to ISIS.[240] The internet is plagued by thousands of terrorist preachings like those of Anwar al-Awlaki, whose name "yields over 70,000 hits" on Google; and videos of the militant leader of Boko Haram, Abubakar Shekau, who was responsible for "5400 religiously and politically motivated attacks in Northern Nigeria" between 2013 and 2015.[241] Proponents of this approach argue that Section 2339(b) will help limit the amount of self-radicalization, lone-wolf-style attacks, and general terrorist content on social media.[242] However, there are complications with applying Section 2339(b) to

---

236. *Id.*

237. *See generally*, Alexander Tsesis, *Terrorist Incitement on the Internet*, 86 FORDHAM L. REV. 367 (2017) [hereinafter *Terrorist Incitement on the Internet*]; Isacson, *supra* note 6.

238. *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 16, at 10 (statement of Honorable Alberto M. Fernandez).

239. *See generally Terrorist Incitement on the Internet*, *supra* note 237, at 377.

240. *Id.* at 370.

241. *Social Media Accountability for Terrorist Propaganda*, *supra* note 164, at 611.

242. *Id.* at 611-13; *see, e.g.*, *Radicalization: Social Media and the Rise of Terrorism*, *supra* note 16, at 8, 10 (statement by Mr. Walter Purdy, president of the Terrorism Research Center);

online social media content. First, there is the issue of the mens rea. A social media company would need to provide material support to an FTO knowingly.[243] It would be incredibly difficult for a social media platform to know the identity of every user. The amount of people that use these social media platforms daily is staggering; in 2019, Facebook had 1.2 billion, and Twitter had 126 million.[244]

It would also be infeasible to expect social media companies like Twitter to run background checks on their users. As seen in the introduction, Facebook attempted to block and "self-censor" posts related to the Christchurch shooting in New Zealand.[245] Self-censorship is practiced by most tech companies in the industry; in 2015, Twitter reported that they removed 125,000 accounts for pro-terrorist content.[246] Some companies, like Facebook, are rewriting their community standards to include "dangerous organizations."[247] These actions show that social media companies are willing and able to self-censor their platforms.[248]

Even if social media companies could identify their users, there would be nothing concrete to base their findings on.[249] Companies would have to rely on the information provided by the user on or about their account.[250] This leads to issues with anonymity, and attribution, as discussed above. In Facebook's terms of service, they ask that a user provide their correct personal information.[251] However, there is nothing compelling or requiring a user to use their real name. How, then, can Facebook truly know who its users are? Furthermore, if they are affiliated with an FTO. Additionally, social media companies would need to be able to assess situations where a user could be coordinating with a Foreign Terrorist Organization "or they [could] be a troubled individual who . . . repost[s] such content gleaned from other internet sources without the requisite coordination."[252] It would be extremely difficult for social media companies to know who exactly its users are and what their agendas are.

If social media companies could identify their users, the next question for the

---

Ruane, *supra* note 186, at 9.

243. 18 U.S.C. § 2339(b)(a)(1).

244. Hamza Shaban, *Twitter Reveals its Daily Active User Numbers for the First Time*, WASH. POST (Feb. 7, 2019), https://www.washingtonpost.com/technology/2019/02/07/twitter-reveals-its-daily-activ?e-user-numbers-first-time/ [https://perma.cc/5SLA-AYJX].

245. *Facebook: New Zealand Attack Video Viewed 4,000 Times*, *supra* note 9.

246. *Twitter Suspends 125,000 'Terrorism' Accounts*, BBC NEWS (Feb. 5, 2016), https://www.bbc.com/news/world-us-canada-35505996 [https://perma.cc/2F6M-44AH].

247. *Id.*

248. *See* Emily Goldberg Knox, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L. J. 295, 314-15 (Dec. 2014).

249. *See generally* Rachel VanLandingham, *Jailing the Twitter Bird*: *Social Media, Material Support to Terrorism, and Muzzling the Modern Press*, CARDOZO L. REV. 1 (Feb. 22, 2017).

250. *See id.* at 39-40.

251. *Terms of Service*, FACEBOOK (JULY 31, 2019), https://www.facebook.com/terms.php [https://perma.cc/PJC7-BUQZ]; s*ee also* VanLandingham, *supra* note 249, at 1.

252. VanLandingham, *supra* note 249, at 42.

courts would be if they provided a service to the FTO that would be considered material support. Under *Holder v. Humanitarian Law Project*, the Supreme Court found that words in "service to," within the statute, must include a connection between the service that is provided and the FTO.[253] Although, the Court did not address the issue of how much coordination equated to "service to" an FTO.[254] As mentioned above, in *United States v. Mehanna*, the court ruled that there is no need for a "direct link" between an FTO and a defendant.

There is a disinterest in criminalizing independent advocacy; *Humanitarian Law Project* and *Mehanna* echo *Brandenburg v. Ohio* in this respect.[255] *Brandenburg* has remained the controlling precedent with respect to the advocacy of violence and lawlessness; and their protection under the First Amendment.[256] The Supreme Court in *Brandenburg* overturned an Ohio criminal syndicalism statute.[257] The statute outlawed "advocate[ing] . . . the duty, necessity or propriety of crime, sabotage, violence, or unlawful methods of terrorism."[258] After a Klu Klux Klan rally that was broadcast in Cincinnati, members were convicted of violating the syndicalism statute.[259] The Klan members made comments that insinuated and advocated for violence: "We're not a revengent organization, but if our President, our Congress, our Supreme Court, continues to suppress the white, Caucasian race, it's possible that there might have to be some revengeance taken."[260] The Court overturned the Ohio statute saying there are:

> "Constitutional guarantees of free speech and free press [that] do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed [at] inciting or producing imminent lawless action and is likely to incite or produce such action."[261]

Brandenburg has been the controlling precedent for courts in dealing with the First Amendment and advocacy of violence since its ruling. However, there is ambiguity in *Brandenburg's* scope of what it means to "likely produce imminent unlawful action."[262] In *Hess v. Indiana*, the Court attempted to clarify this ambiguity by noting that violence that will occur in "some indefinite future time" is not enough to shed First Amendment protections.[263]

Humanitarian Law Project and, especially, *Mehanna*, could be seen to help

---

253. Holder v. Humanitarian Law Project, 561 U.S. 1, 30 (2010).

254. *Id.*

255. *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 448 (1969); Ruane, *supra* note 186, at 3.

256. *See* Ruane, *supra* note 186, at 4.

257. *Brandenburg*, 395 U.S. at 444 (1969).

258. *Id.* at 444-45; *see also.* Ruane, *supra* note 286, at 4.

259. *Brandenburg*, 395 U.S. at 445.

260. *Id.* at 446.

261. *Id.* at 447.

262. *See* Ruane, *supra* note 186, at 4. *See generally* Buchhandler-Raphael, *supra* note 181, at 1678-80.

263. Hess v. Indiana, 414 U.S. 105, 108 (1973).

those who advocate for Section 2339(b). However, following the First Amendment considerations, the use of Section 2339(b) to prosecute social media companies for their alleged material support of FTOs, would be difficult. The question that would need to be answered would be how much coordination is needed to prosecute an individual. *Humanitarian Law Project* left the question of coordination between an FTO and defendant open. While *Mehanna* articulated that there is no need for a "direct link" in coordination, as mentioned above, there still needs to be some semblance of a link. The hurdles that using Section 2339(b) would put before a court and social media companies make it an unlikely and unproductive choice in fighting online terrorist content.

IV. A WAY FORWARD: RECONCILING NATIONAL SECURITY AND THE CONSTITUTION

The threat of online terrorist content has presented the United States, as well as the world, with the complex problem of balancing fundamental rights, like free speech, with national security concerns. The two concerns are intertwined and yet irreconcilable. The laws discussed above from the United States and the European Union try to balance these competing interests. The European Union has taken a firmer national security stance, identifying the urgent need to stop terrorist content on social media. The proposed EU regulation is unlike anything the United States currently has. The United States must contend with the Constitutional guarantee of free speech under the First Amendment. The laws that are currently on the books place a strong emphasis on protecting free speech and freedom of expression. Laws like Section 230 of the Communications Decency Act are thought to be the bedrock of Internet freedom. However, the Internet freedom that millions of Americans have enjoyed has also allowed a more sinister force to take root. Terrorist content online has flourished under the American pillars of the First Amendment. The best way to straddle the line between national security and First Amendment concerns would be to create a narrowly defined exception within Section 230 of the Communications Decency Act.

As mentioned above, Congress created the FOSTA exception within Section 230 in 2018.[264] The exception aims to help fight human trafficking online.[265] Rather than mandating that tech companies censor and monitor content related to human trafficking, the exception removes Section 230 as a defense.[266] Thus, forcing tech companies to censor their platforms to prevent themselves from being sued. The broad application of the CDA has allowed companies to have free reign over whether and how they want to monitor and censor social media content. As the introduction to this Note discussed, the Christchurch shooting was live-streamed on Facebook, and it was not reported until 12 minutes *after* it ended.[267] And "within 24 hours, [Facebook] had blocked 1.2 million copies at the

264. Brannon, *supra* note 210, at 3.

265. *Id.*

266. *Id.*

267. *Facebook: New Zealand Attack Video Viewed 4,000 Times*, *supra* note 9 (emphasis

point of upload" and it was viewed more than 4,000 times before it was removed.[268] It has been months since the attack, and footage and related content of the shooting are still being found by Facebook.[269] It shows the difficulty and incapability of social media companies to prevent the spread of terrorist content on their platforms.

An exception within the CDA could help motivate social media companies to be more proactive in their detection of terrorist content. However, the threat of litigation could spur companies to remove any content that has any resemblance to terrorist content. In regards to regulating the internet, many have cautioned the government that regulating "certain types of content, viewpoints, or speakers . . .could lead to serious First Amendment concerns."[270] For example, in 1997, the Supreme Court struck down an addition to the CDA that would have "made it a crime to send "indecent" or "patently offensive" messages to children, concluding that these prohibitions were too vague and violated the First Amendment."[271]

However, these First Amendment concerns and the concern of vagueness within a CDA exception could be eliminated or at least alleviated with a narrow definition of what terrorist content is. In *Woodhull Freedom Foundation v. United States*, the Supreme Court dismissed a claim arguing that FOSTA civilly and criminally penalizes protected speech when it holds online service providers liable for "promot[ing] or facilitat[ing]" prostitution. However, in the dicta, the Court narrowed the definitions of promoting and facilitating. This lessened the First Amendment concerns, and the same could be done for a terrorist content exception.[272]

To better confine and prevent over removal by social media platforms, this Note advocates for an exception that would be predicated on social media companies not acting after a series of conditions. Much like the EU Terrorist Content Regulation works on a referral system, so too would this CDA exception. However, rather than companies being penalized for systematic failure to take down the offensive content, American companies would have their Section 230 immunity stripped. These conditions would act as a system of referrals altering companies to terrorist content.

The first condition would be that companies find the terrorist content themselves. This would allow companies to continue to monitor their own platforms for terrorist content and avoid direct government regulation of social media. Thus, avoiding tricky First Amendment violations. Unlike the EU Internet Forum, which allowed for the public to report terrorist content, this exception would not have a condition predicated on users' referring content. The main goal of this exception is to identify and remove terrorist content in the most efficient way. Having companies being held responsible for the alertness of their users is

---

added).

268. *Id.*

269. Uberti, *supra* note 12.

270. Brannon, *supra* note 210, at 4.

271. *Id.*

272. *Id.*

not only unfair, but it could also potentially waste valuable time and resources. This exception would require social media companies to set aside more employees and resources to identify and respond to terrorist content in order to avoid possible litigation. Having these employees investigate every referral by a user would be time-consuming and could potentially lead to wasted time and resources.

The second condition would be a referral by law enforcement. This would happen either because the social media company failed to or missed identifying the content as terrorist-related content. This would be the last chance for companies to catch and remove offending content or user. Who would constitute "law enforcement" could be those entities established under Section 201 of the Homeland Security Act of 2002.[273] These are the federal agencies that have access to the public and private information shared under the Cybersecurity Information Sharing Act of 2015 ("CISA").[274] The Cybersecurity Information Sharing Act was enacted to "help combat hackers and reduce the fallout from these catastrophic data breaches that have exposed hundreds of millions of Americans' personal information in the last few years."[275] The Act was created to allow Internet providers to voluntarily share information with the government in the hopes of reducing the number of cyber-attacks and online terrorism. In regard to CISA, the use of these entities allows "them to analyze any potential "'terrorist threats to the homeland' and 'actual and potential vulnerabilities to the homeland.'"[276] The same entities could be used under this Note's proposed CDA exception. They would be in the best position to alert social media companies to potential terrorist content on their platforms. If social media companies fail to remove content after being alerted by law enforcement, their CDA immunity would be removed.

Once social media companies are alerted to potential terrorist content, they would have a limited time to respond and either take down the offending content or object. As with the European Union's Terrorist Content Regulation, the time frame is essential. The EU proposal has a one-hour time limit.[277] For many opponents of the proposed EU regulation, this is one of their main concerns. The one-hour time limit is thought to be too burdensome on small businesses and almost impractical.[278] A more flexible time frame would allow for social media

---

273. Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, CONG. RSCH. SERV. 6 (Mar. 16, 2015), https://fas.org/sgp/crs/intel/R43941.pdf [https://perma.cc/SSL9-2A97].

274. *Id.*

275. Cory Bennett, *Congress Approves First Major Cyber Bill in Years*, THE HILL (Dec. 18, 2015), https://thehill.com/policy/cybersecurity/263696-congress-approves-first-major-cyber-bill-in-years [https://perma.cc/MHJ7-LLEL].

276. Nolan, *supra* note 273, at 6.

277. *Commission Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online*, at 4, COM (2018) 640 final (Dec. 12, 2018).

278. Hoboken et al., *supra* note 65, at 2.

companies to properly investigate if they identified the content and/or to come up with the proper plan to remove and prevent content from being re-uploaded. More research would need to be done to set a proper time frame for removal.

However, using the Communications Decency Act to prevent the dissemination of terrorist content may not have that much effect on terrorist radicalization. In 2015, social media companies adopted a harder approach to removing terrorist content. They began using artificial intelligence and "dedicated teams" to eliminate posts. However, terrorist groups also began to change their online tactics. They manipulated social media platforms by posting material that went up to but did not cross the line of being flagged by users or outside observers. Many of the groups also use proxies, such as media organizations or local charities, to post content on the platforms for them. Hezbollah has no official accounts; however, they have a considerable presence online. For example, a broadcaster with strong ties to Hezbollah, Al Manar, has 481,000 followers. Many of the videos associated with Al Manar "have tens of thousands of views and have been on the site for years."[279] Hamas has a similar online presence with an Instagram for its television station, Al Aqsa, and a Twitter feed for the group. There can be an argument made that any online monitoring of terrorist content will not be enough to prevent terrorist propaganda.

To properly alleviate this potential roadblock to fighting the dissemination of terrorist content on social media, there needs to be a level of cooperation between the social media companies and the federal government. Congressman Max Rose, the Chair of the Homeland Security Subcommittee on Intelligence and Counterterrorism, stated, "Social media companies have become instructions in our society and have a responsibility to stop the spread of terrorist content on their platforms . . . [however] the reality is we all need to work together—private companies, non-profit and research institutions, and the federal government."[280] In order to accomplish this cooperation, the government and law enforcement should work with social media companies to come up with proper terrorist content indicators. With CISA, the government is required to share its "cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses."[281] The proposed CDA exception could have the same level of cooperation. This way social media companies can better identify and remove terrorist content.

Similar to the proposed EU regulation, social media companies should make law enforcement aware of the content they are finding and/or removing when it

---

279. Sheera Frenkel & Ben Hubbard, *After Social Media Bans, Militant Groups Found Ways to Remain*, N.Y. TIMES (Apr. 19, 2019), https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html [https://perma.cc/Z5ZL-T9MD].

280. *Rose Introduces Raising the Bar Act to Address Terrorist Content on Social Media*, COMM. HOMELAND SEC. (Nov. 21, 2019), https://homeland.house.gov/news/legislation/rose-introduces-raising-the-bar-act-to-address-terrorist-content-on-social-media [https://perma.cc/7D7H-QPUQ].

281. John Heidenreich, *The Privacy Issues Presented by the Cybersecurity Information Sharing Act*, 91 N.D. L. REV. 394, 400 (2015).

poses a risk to safety or life. Using an approach like this Note's recommendation would also continue to provide information to counterterrorism agencies.[282] As Martin Libicki, a senior policy analyst at the RAND Corporation, stated, "You can learn a lot from the enemy by watching them online."[283] Along with sharing information with the government, social media companies should also be required to share information with fellow social media companies. This would allow social media companies to create an information network to better identify potential FTOS and those that are affiliated with them.

CONCLUSION

As the number of terrorist groups using social media platforms to spread their hateful messages and radicalize new followers, the United States needs to look to more effective ways of stopping the dissemination of terrorist content. Terrorist groups have been able to spread their message far and wide. In 2014, before ISIS captured Mosul, Iraq, "it rolled out an extensive online campaign with text, images, and videos that threatened the city's residents with unparalleled death and destruction."[284] It is actions such as these that have caused many lawmakers and citizens to call on the government to prevent these acts. This Note proposes that a conditional exception in Section 230 of the Communications Decency Act would be the most effective way to stop the dissemination of terrorist content on social media. The United States can look to the European Union and its EU Internet Forum and the newly proposed Terrorist Content Regulation. However, as this Note discusses, the United States must stay in line with the First Amendment and the Constitution. Thus, the United States cannot properly promulgate a law like the Terrorist Content Regulation. To prevent a violation of the First Amendment and to also combat the growing threat of terrorist content online, an exception within the CDA must be created. This will allow Americans and the judicial system to hold social media companies accountable for their failure to stop the dissemination of terrorist content. The exception would be a conditional exception, where social media companies would be given a chance to remedy the situation if they failed to identify the terrorist content. After a more flexible time frame than the EU's one-hour rule, the company would then lose its immunity shield from the CDA. This exception would then allow a more cooperative partnership between the federal government and private social media companies.

---

282. Ariel V. Lieberman, *Terrorism, the Internet, and Propaganda: A Deadly Combination*, 9 J. NAT'L SEC. L & POL'Y 95, 117, 123 (2017).

283. Frenkel & Hubbard, *supra* 279.

284. Jared Cohen, *Digital Counterinsurgency: How to Marginalize the Islamic State Online*, FOREIGN AFFS. (Nov/Dec 2015), https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency [https://perma.cc/T9SQ-RLF3].