Fordham Law Review

Volume 86 | Issue 2 Article 12

2017

Social Media Accountability for Terrorist Propaganda

Alexander Tsesis
Loyola University School of Law

SOCIAL MEDIA ACCOUNTABILITY FOR TERRORIST PROPAGANDA

*Alexander Tsesis**

Terrorist organizations have found social media websites to be invaluable for disseminating ideology, recruiting terrorists, and planning operations. National and international leaders have repeatedly pointed out the dangers terrorists pose to ordinary people and state institutions. In the United States, the federal Communications Decency Act's § 230 provides social networking websites with immunity against civil law suits. Litigants have therefore been unsuccessful in obtaining redress against internet companies who host or disseminate third-party terrorist content. This Article demonstrates that § 230 does not bar private parties from recovery if they can prove that a social media company had received complaints about specific webpages, videos, posts, articles, IP addresses, or accounts of foreign terrorist organizations; the company's failure to remove the material; a terrorist's subsequent viewing of or interacting with the material on the website; and that terrorist's acting upon the propaganda to harm the plaintiff.

This Article argues that irrespective of civil immunity, the First Amendment does not limit Congress's authority to impose criminal liability on those content intermediaries who have been notified that their websites are hosting third-party foreign terrorist incitement, recruitment, or instruction. Neither the First Amendment nor the Communications Decency Act prevents this form of federal criminal prosecution. A social media company can be prosecuted for material support of terrorism if it is knowingly providing a platform to organizations or individuals who advocate the commission of terrorist acts. Mechanisms will also need to be created that can enable administrators to take emergency measures, while simultaneously preserving the due process rights of internet intermediaries to challenge orders to immediately block, temporarily remove, or permanently destroy data.

* Raymond & Mary Simon Chair in Constitutional Law and Professor of Law, Loyola University School of Law, Chicago. Thanks are due to Jack Balkin, Richard Bierschbach, Danielle Citron, and Martin Redish. This Article was prepared for the *Fordham Law Review* symposium entitled *Terrorist Incitement on the Internet* held at Fordham University School of Law. For an overview of the symposium, see Alexander Tsesis, *Foreword: Terrorist Incitement on the Internet*, 86 FORDHAM L. REV. 367 (2017).

INTRODUCTION

Audiences worldwide rely on web services to access a wide variety of content. Internet information channels transmit everything from historical documents, music videos, and political blogs to defamatory statements, bomb-making instructions, torture videos, and child abuse recordings. Terrorist groups have found the internet to be a godsend, offering an effective platform for developing social bonds, radicalizing recruits, and increasing membership.[1] Coordinated terrorist missions can be planned from afar, as recently occurred in India, where engineer Mohammed Ibrahim Yazdani and his terrorist cohorts received and unsuccessfully conspired to act on directives to attack technical infrastructures.[2] His Islamic State handlers sent digital instructions to him from Syria and orchestrated an elaborate plot for obtaining weapons and explosive chemicals.[3] Even before he began actively participating in the terror plot, Yazdani was won over by "the Islamic State's online propaganda."[4]

Parties who seek legal redress for injuries perpetrated by individuals indoctrinated through internet advocacy often encounter legal barriers. This is especially conspicuous in lawsuits filed against web services hosting objectionable content, such as terrorist incitement and related information. Internet service providers (ISPs), online service providers, search engines, and social networking websites commonly invoke § 230 of the Communications Decency Act (CDA) to assert immunity from civil lawsuits.[5] District and appellate courts have consistently ruled in favor of

1. HOMELAND SECURITY INSTITUTE, THE INTERNET AS A TERRORIST TOOL FOR RECRUITMENT AND RADICALIZATION OF YOUTH 6 (2009), http://barakaconsult.com/uploads/reports%20on%20internet_radicalization.pdf [https://perma.cc/2K65-62QQ].

2. Rukmini Callimachi, *Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots from Afar*, N.Y. TIMES (Feb. 4, 2017), https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html [https://perma.cc/CA6E-S5LW].

3. *Id.*

4. *Id.*

5. *See* Klayman v. Zuckerberg, 753 F.3d 1354, 1357 (D.C. Cir. 2014) (finding that a social networking website like Facebook is immune under the CDA); Getachew v. Google, Inc., 491 F. App'x 923, 925–26 (10th Cir. 2012) (holding that an internet search engine is immune from litigation alleging harm to reputation resulting from information discovered through an internet search); Black v. Google, Inc., 457 F. App'x 622, 623 (9th Cir. 2011) (finding that an ISP is immune from defamation litigation); Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010) (holding that the CDA bars "plaintiffs from holding ISPs legally

defendants relying on this strategy. Litigants have unsuccessfully sought redress from internet companies for hosting and disseminating third-party terrorist and defamatory contents.[6]

Congress intended § 230 immunity to preserve robust communications and to place responsibility on information intermediaries to take down harmful communications.[7] The underlying aims arose from First Amendment concerns and bureaucratic considerations; however, the approach has become a strategic arrow in the quivers of web companies seeking to limit liability from knowingly allowing foreign terrorist organizations to exploit digital platforms to recruit and threaten. Digital information companies have seized on a law created to advance robust internet communications to shield their businesses from liability for refusing to eliminate all threatening videos and messages.

The policy of immunizing digital social media has some clear benefits: facilitating the spread of ideas, democratic values, creativity, culture, art, friendship, travel, news, and much more. Moreover, it is arguably in keeping with the U.S. Supreme Court's aversion to content-based restrictions on expression,[8] especially preventing parties from being subject to suits for third parties' fraudulent or illegal postings about which the intermediary remained unaware.[9] However, certain heinous content on the internet, especially terrorist propaganda, raises compelling public concerns. Just as online information intermediaries are not immune from criminal liability, neither should they enjoy immunity from civil lawsuits. The United Nations Office on Drugs and Crime has made clear the international import of having the United States take legislative initiative by passing a statute to combat terrorist propaganda: "It would be extremely helpful to other countries if the United States could find a solution to its limited ability to furnish judicial cooperation concerning foreign incitement offenses resulting from its jurisprudence concerning freedom of speech and expression."[10] Even as litigants remain hampered in their abilities to obtain civil redress for harms, the Justice Department can file criminal charges against social media companies that knowingly host foreign terrorist organizations.[11]

---

responsible for information that third parties created and developed"); Whitney Info. Network, Inc. v. Verio, Inc., No. 2:04CV462FTM29SPC, 2006 WL 66724, at *3 (M.D. Fla. Jan. 11, 2006) (determining that a web hosting service was immune from liability under the Communications Decency Act because it hosted an allegedly offending website but did not create its contents).

6. *See, e.g.*, Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003) ("[Section] 230 limits immunity to information 'provided by another information content provider.' An 'information content provider' is defined by the statute to mean '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.'" (quoting 47 U.S.C. § 230 (2012)).

7. David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 410 (2010); Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1142 (2005).

8. Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226 (2015).

9. Smith v. California, 361 U.S. 147, 153–54 (1959).

10. U.N. OFFICE ON DRUGS & CRIME, DIGEST OF TERRORIST CASES 118 (2010).

11. *See infra* Part III.B.

This Article argues that irrespective of civil immunity, the First Amendment does not limit Congress's authority to impose criminal liability on those content intermediaries who have been notified that their websites are hosting third-party foreign terrorist incitement, recruitment, or instruction. Neither the First Amendment nor the CDA prevents this form of federal criminal prosecution. Gaining clarity about the constitutional issues involved is consequential because, to date, the government has failed to bring suit against internet information companies such as Twitter, Facebook, and Google for material support of terrorists.

Part I of this Article details the uses of social media sites to disseminate terrorist materials. Part II elaborates the relevant First Amendment limitations pertinent to the regulation of intermediaries who carry and publicly make available terrorist materials on their websites. Part III first discusses CDA immunity from civil litigation. It then explains how federal criminal law can and should hold digital intermediaries responsible for hosting terrorist-sponsored, terrorist-initiated, or terrorist-controlled digital materials. The refusal to either notify law enforcement authorities or to take down the offending materials poses national and local threats to safety and security.

I. TERRORIST FORUMS ON SOCIAL MEDIA

Over the last ten years, social media websites have become critical tools for the dissemination of terrorist propaganda. A number of terrorists, including Omar Mateen, who attacked the Pulse gay nightclub in Orlando, Florida, murdering forty-nine people and injuring fifty-three others, were radicalized in part through digital materials readily available on the internet.[12] The Islamic State of Iraq and Syria (ISIS), Hamas, and a variety of other terrorist organizations use Facebook to recruit and to propagandize.[13] Al Qaeda, Hezbollah, and Minbar al-Tawhid wal-Jihad are among the groups who have found Twitter to be tremendously helpful for spreading messages of political violence and group hatred.[14] YouTube, another major social media intermediary on which third parties rely to circulate all manner of instructional, entertainment, and private video content, is also a hub of terrorist indoctrination and teaching.[15] These companies make radical clips digitally available throughout the world, enabling terrorist leaders to affect the conduct of millions of viewers. Terrorist associations have found Twitter

12. Ed Pilkington & Dan Roberts, *FBI and Obama Confirm Omar Mateen Was Radicalized on the Internet*, GUARDIAN (June 14, 2016), https://www.theguardian.com/us-news/2016/jun/13/pulse-nightclub-attack-shooter-radicalized-internet-orlando [https://perma.cc/7MLL-Q3W6].

13. *See* Abigail Tracy, *Facebook's $1 Billion Terrorism Lawsuit Points to a Huge Problem for Silicon Valley*, VANITY FAIR (July 12, 2016), http://www.vanityfair.com/news/2016/07/facebook-billion-dollar-terrorism-lawsuit [http://perma.cc/W9W3-DSTW]; Dan Warburton, *British ISIS Leader "Using Facebook to Recruit Terrorists to Target the UK,"* MIRROR (Mar. 12, 2016), http://www.mirror.co.uk/news/uk-news/british-isis-leader-using-facebook-7545645 [https://perma.cc/6YWD-9Q3D].

14. GABRIEL WEIMANN, TERRORISM IN CYBERSPACE: THE NEXT GENERATION 139 (2015).

15. *Id.* at 141–46.

and YouTube to be invaluable forums for amplifying and disseminating violent propaganda and information. In addition, national security experts have warned that those platforms can even be manipulated to orchestrate real-time operations, which empowers handlers to direct attacks either from distant shores or in close proximity.[16]

Many internet information companies post written policies against using their platforms to spread violence and hatred, but their staffs are often intransigent, even upon receipt of credible information about overt violent instigation on their websites.[17] While social media companies remove some terrorist content, they often deny watchdog requests, even after being alerted that posts overtly advocate the use of violence to achieve a social or political end.[18] Advocacy groups have periodically found it difficult or impossible to convince social media companies to remove online terrorist communications.[19] Indeed, in many cases, companies like Facebook have allowed degrading statements to be accessed on their platforms despite their own standards for community decency.

Facebook pledges to remove "graphic images when they are shared for sadistic pleasure or to celebrate or glorify violence."[20] Although its administrators received several requests to take down a graphic page called "Stab Israelis," Facebook refused to abide by its written policy against posting statements favoring brutal attacks.[21] Not only was the title of that website an explicit instigation to violence, but the images on it clearly depicted background images with a Palestinian flag and a superimposed male hand holding a large butcher knife.[22] Likewise, Facebook found that a page called "Death to Zionst [sic] baby killer Israeli Jews" did not violate its community standard against hate speech.[23] Nor were these isolated failures to respond.

---

16. Steven Muslin, *U.S. Army Warns of Twittering Terrorists*, CNET (Oct. 28, 2008), https://www.cnet.com/news/u-s-army-warns-of-twittering-terrorists/ [https://perma.cc/7VNF-LHBV].

17. *See infra* note 21.

18. *See infra* note 22.

19. Scott Shane, *Internet Firms Urged to Limit Work of Anwar al-Awlaki*, N.Y. TIMES (Dec. 18, 2015), https://www.nytimes.com/2015/12/19/us/politics/internet-firms-urged-to-limit-work-of-anwar-al-awlaki.html [https://perma.cc/4Q9R-SQ4H].

20. *Community Standards: Encouraging Respectful Behavior*, FACEBOOK, https://www.facebook.com/communitystandards#violence-and-graphic-content [https://perma.cc/2FRH-HQ9T] (last visited Oct. 16, 2017).

21. Yitzhak Benhorin, *20,000 Israelis Sue Facebook*, YNETNEWS.COM (Oct. 27, 2015), http://www.ynetnews.com/articles/0,7340,L-4716980,00.html [https://perma.cc/8W3Y-GREV]. While Facebook initially refused to eliminate the "Stab Israelis" page, it eventually complied after an Israeli newspaper printed information about the company's intransigence. JNS.org, *Facebook Removes 'Stab Israelis' Page Following Article in Hebrew Press*, ALGEMEINER (Oct. 14, 2015, 2:46 PM), http://www.algemeiner.com/2015/10/14/facebook-removes-stab-israelis-page-following-article-in-hebrew-press/ [https://perma.cc/L8AS-SERV].

22. *See* JNS.org, *supra* note 21.

23. *"Death to Zionist Baby Killer Israeli Jews" Is OK on Facebook*, BEFORE IT'S NEWS (July 28, 2014, 10:03 AM), http://beforeitsnews.com/opinion-conservative/2014/07/death-to-zionist-baby-killer-israeli-jews-is-ok-on-facebook-2886068.html [https://perma.cc/T6JZ-YJ9X].

Facebook likewise refused to censor anti-Muslim hate websites. Despite receiving reports of at least fifty offending pages, some instigating violence, the company refused to take down many inciteful sites.[24] The latter Facebook pages incite against Muslims through the uses of stereotyping, dehumanizing statements, and advocacy for their exclusion from civil society.[25] Other groups who have long been the targets of hatred, such as the Roma and Sinti, also face violent online calls for their geographic displacement.[26] The list of targeted groups could be extended to many other identifiable communities.

Especially violent language is found on many anti-Semitic forums. For example, a Facebook page contained a graphic painting showing a man walking menacingly, shoulders hunched, down the street with a butcher knife in his hand in the direction of two Chasidic Jews at a bus stop.[27] These pages appeared during a spate of terrorist stabbings in Israel.[28] They were not merely parodies or oppositional statements but among a plethora of Facebook pages that praised and urged anti-Semitic violence. "There is nothing greater than a knife penetrating the heads of the Jews," read another page.[29] In a separate post, a teacher at one of the United Nations Relief and Works Agency (UNRWA) schools posted a call to "hit Tel Aviv . . . Screw the Jews hahaha," to the side of a digital photo that depicted a man shooting a rocket launcher with explosives detonating near him.[30] Another UNRWA teacher's Facebook page asserted, "Good news to the Zionist settlers, choose your preferred method of death, and we will provide it. Run over, knife, screw, axe, hammer, choke, hang, skinning, cutting."[31] Facebook's failure to abide by its contractual terms of decency puts into serious doubt whether the current regimen of relying on corporate self-policing suffices. Regulations are needed that would require Facebook actively to review its databases for the presence of terrorist speech, to remove it even in the absence of third-party complaints, and to monitor ISP addresses from which hateful or inciteful materials had been sent. Criminal liability, as this Article argues in

24. *How Facebook Responded to Anti-Muslim Hate*, ONLINE HATE PREVENTION INST. (Dec. 8, 2014), http://ohpi.org.au/how-facebook-responded-to-anti-muslim-hate/ [https://perma.cc/GEH2-4AZH].

25. Andre Oboler, *The Normalisation of Islamophobia Through Social Media: Facebook*, *in* ISLAMOPHOBIA IN CYBERSPACE: HATE CRIMES GO VIRAL 41, 45 (Imran Awan ed., 2016).

26. *Anti-Roma Violence Highlights Need for Better Online Hate Speech Laws*, NASC (Nov. 6, 2014), http://www.nascireland.org/latest-news/anti-roma-violence-highlights-need-better-online-hate-speech-laws/ [https://perma.cc/BS29-CRZH].

27. *Social Media as a Platform for Palestinian Incitement—Praise for Stabbing Attackers, Threats of Further Attacks*, MIDDLE E. MEDIA RES. INST. (Oct. 14, 2015), https://www.memri.org/reports/social-media-platform-palestinian-incitement-praise-stabbing-attackers-threats-further [https://perma.cc/4YSV-XZUY].

28. Ben Wedeman, *Israeli-Palestinian Violence: What You Need to Know*, CNN (Oct. 15, 2015, 12:32 PM), http://edition.cnn.com/2015/10/14/middleeast/israel-palestinians-violence-explainer/ [https://perma.cc/S2WV-FPWE].

29. Lawrence J. Haas, *Sowing the Seeds of More Mayhem*, U.S. NEWS (Oct. 20, 2015, 12:30 PM), http://www.usnews.com/opinion/blogs/world-report/2015/10/20/western-response-to-palestinian-violence-encourages-more-terror [https://perma.cc/R5S4-SBYL].

30. UN WATCH, POISONING PALESTINIAN CHILDREN 13 (2017).

31. *Id.* at 79.

Part III, would be the most effective means of addressing the dissemination of extremist digital communications.

The offending materials are not merely offensive and degrading. Facebook has become an important conduit through which terrorists to communicate and inspire audiences. One of the two spouses who committed mass terrorism in San Bernardino, Tashfeen Malik, announced her allegiance to ISIS through a Facebook post.[32] Given the sophistication of Facebook algorithms, which are capable of producing almost immediate targeted advertisement to persons posting on its platform,[33] it is conceivable that a refined algorithm can be designed to quickly identify posts supporting terrorism.

Terrorist preaching on other sources is not at all subtle and is easily identifiable. Terrorist videos are plentiful on YouTube. A simple search of Anwar al-Awlaki's name on the website yields over 70,000 hits.[34] Al-Awlaki, who was assassinated by the United States in Yemen, was a notorious propagandist with a vast following.[35] Before Malik and her husband, Syed Farook, participated in the mass shooting at a community center, they had listened to hours of al-Awlaki's inciteful lectures.[36]

YouTube also hosts videos of Abubakar Shekau, the militant leader of the Boko Haram terrorist group that between 2013 and 2015 was responsible for about 5400 religiously and politically motivated attacks in northern Nigeria.[37] Al-Awlaki's and Shekau's videos are a collage of indoctrination, degradation, propagandization, and recruitment.[38] Requests that YouTube voluntarily remove al-Awlaki's videos have enjoyed limited success.[39] With

---

32. Richard A. Serrano, *Tashfeen Malik Messaged Facebook Friends About Her Support for Jihad*, L.A. TIMES (Dec. 14, 2015, 5:41 PM), http://www.latimes.com/local/lanow/la-me-ln-malik-facebook-messages-jihad-20151214-story.html [https://perma.cc/4SK3-E4AX].

33. *Targeting Audiences*, FACEBOOK FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/audiences-api [https://perma.cc/PG79-34BQ] (last visited Oct. 16, 2017).

34. *Search Results*, YOUTUBE, https://www.youtube.com/results?search_query=anwar+al-awlaki [https://perma.cc/PV44-HT4X] (last visited Oct. 16, 2017).

35. Marc Ginsberg, *Urgent Call to Action: You Tube Must Cease Abetting Terrorism in the U.S.*, HUFFINGTON POST (June 21, 2016, 2:39 PM), http://www.huffingtonpost.com/amb-marc-ginsberg/urgent-call-to-action-you_b_10595574.html [https://perma.cc/N5QH-TV6D].

36. Shane, *supra* note 19.

37. Jason Nichols, *Boko Haram Is as Big a Threat as ISIS. So Why Are We Ignoring It?*, HILL (Jan. 18, 2017, 1:00 PM), http://thehill.com/blogs/pundits-blog/international-affairs/314807-boko-haram-is-as-big-as-threat-as-isis-why-are-we [https://perma.cc/U2AF-DNCR].

38. Mark D. Wallace, *Remove Terrorists from YouTube: Column*, USA TODAY (Jan. 25, 2016, 7:33 AM), http://www.usatoday.com/story/opinion/2016/01/25/remove-terrorists-youtube-social-media-column/78939982/ [https://perma.cc/9XVA-HJBJ]. For examples of Boko Haram videos with English transcription see Samuel Lewis, *Boko Haram Release Chilling Videos of Missing Nigerian Schoolgirls—with Subtitles*, YOUTUBE (May 12, 2014) https://www.youtube.com/watch?v=MmL2T9r0QbM [https://perma.cc/SH3G-KVCB]; splashnaijaNG, *Scary Stuff! Full Transcript of Shekau's Recently Released Boko Haram Video*, YOUTUBE (Nov. 1, 2014), https://www.youtube.com/watch?v=zf3SDizT6x8 [https://perma.cc/2CPB-5U6C].

39. *See* James Gordon Meek & Kenneth R. Bazinet, *YouTube's Got to Gag Jihad Mouthpiece Anwar al-Awlaki: Rep. Anthony Weiner*, N.Y. DAILY NEWS (Oct. 24, 2010), http://www.nydailynews.com/news/national/youtube-gag-jihad-mouthpiece-anwar-al-awlaki-rep-anthony-weiner-article-1.187619 [https://perma.cc/4WNN-9BYS].

no legal consequences threatening its operations, YouTube has steadfastly refused requests to remove all videos of international terrorists from its searchable database, despite their highly inciteful and intentionally threatening contents.

That social media company has also rebuffed customer takedown requests for the extremist videos of Anjem Choudary, who called on his followers to join ISIS and praised the martyrdom of the September 11 hijackers.[40] Some videos are taken down for violating the community guidelines,[41] but the company is selective and nontransparent about its decisions. Even after Choudary reportedly influenced over 100 people to commit acts of terrorism and was sentenced to five-and-a-half years in jail,[42] his followers have continued to upload and watch his sermons on YouTube.[43] Twitter also allows Choudary to spread his ideas, where he has tens of thousands of followers, but British police requests to delete that account went unanswered.[44]

Terrorist organizations have widespread presence on prominent social media websites. Terrorists use digital platforms to spread ideology, recruit, and legitimize violent political schemes. Information providers have indirectly contributed to the unprecedented spread of radical calls for ideological and religious murder, war, and enslavement. Without regulatory intervention, web platforms are likely to continue aiding these organizations in enlisting new disciples.

The threat terrorist organizations pose to stability, public safety, and national security is widespread and should be addressed by government initiatives. The European Commission has warned, "[T]errorist groups have demonstrated advanced skills in the use of the internet and new

---

40. Vikram Dodd, *Anjem Choudary Jailed for Five-and-a-Half Years for Urging Support of Isis*, GUARDIAN (Sept. 6, 2016, 1:36 PM), https://www.theguardian.com/uk-news/2016/sep/06/anjem-choudary-jailed-for-five-years-and-six-months-for-urging-support-of-isis [https://perma.cc/5W9P-SYXU]. For video examples of his teachings, see Liberalisten1995, *Anjem Choudary Speaks Out [Big Interview]*, YOUTUBE (July 1, 2014), https://www.youtube.com/watch?v=PJENp68YBKY [https://perma.cc/JMU9-H6AS]; Y.O.Y., *Anjem Choudary Muslim Hate Speech*, YOUTUBE (Aug. 9, 2016), https://www.youtube.com/watch?v=RsUBk11q92U [https://perma.cc/WKJ9-YNFA].

41. Emily Pennink, *Anjem Choudary Verdict: YouTube and Twitter Refused to Delete Radical Preacher's Extremist Posts, Court Hears*, INDEPENDENT (Aug. 16, 2016), http://www.independent.co.uk/news/uk/crime/anjem-choudary-verdict-youtube-twitter-facebook-isis-terrorism-posts-not-deleted-a7194041.html [https://perma.cc/73QZ-8ZWY].

42. Michael Adebolajo, who participated in the murder of the soldier Lee Rigby, was one of those whom Choudary influenced to commit terrorism. Vikram Dodd & Jamie Grierson, *Revealed: How Anjem Choudary Influenced at Least 100 British Jihadis*, GUARDIAN (Aug. 16, 2016, 1:14 PM), https://www.theguardian.com/uk-news/2016/aug/16/revealed-how-anjem-choudary-inspired-at-least-100-british-jihadis [https://perma.cc/6259-FMQR].

43. Joseph Curtis, *Outrage as Extremist Hate Videos Starring Hate Preacher Anjem Choudary's Followers Are STILL on YouTube Despite His Conviction*, DAILY MAIL (Aug. 20, 2016, 11:17 PM), http://www.dailymail.co.uk/news/article-3750223/Outrage-extremist-hate-videos-starring-hate-preacher-Anjem-Choudary-s-followers-available-online-despite-jailing.html [https://perma.cc/6SF7-ZURS].

44. Press Association, *Twitter and YouTube Would Not Remove Anjem Choudary's Posts, Court Told*, GUARDIAN (Aug. 16, 2016, 12:33 PM), https://www.theguardian.com/media/2016/aug/16/twitter-youtube-anjem-choudary-social-media [https://perma.cc/2EHB-XBAC].

communication technologies to disseminate propaganda, interact with potential recruits, share knowledge, plan and coordinate operations."[45] Corporate self-policing is a start, but, by itself, reliance on private actors is insufficient to deal with a problem of such widespread magnitude. Social media companies' initiatives have been insufficient to remove tens of thousands of posts, videos, accounts, and texts. Mandatory schemes should be developed requiring digital information providers to transmit suspicious posts to a central cyberterror unit, which can examine the material and refer First Amendment questions to agency counsel or the attorney general's office.[46]

II. FIRST AMENDMENT CONCERNS

Statutes regulating social media responsibility for inciteful messages posted by third parties raise First Amendment concerns about how to maintain national security while safeguarding free expression. Adjudication should balance government's obligation to combat terrorism with the personal right to enjoy uncensored information. The Supreme Court has found that under ordinary circumstances government may not impose absolute restrictions on the contents of speech.[47]

This judicial finding has not, however, been understood as an absolute bar to regulation. Some narrowly tailored censorship is appropriate, especially where there is the compelling public reason to punish intentionally seditious calls to engage in armed violence.[48] The Court has in addition found speech that is obscene to be outside the purview of the First Amendment. The test for obscenity is overtly content based, allowing the trier of fact to examine whether, "taken as a whole," statements or pictorial depictions have "serious literary, artistic, political, or scientific value."[49] Words that are likely to illicit an "immediate breach of the peace," such as a fight, are likewise unprotected.[50] Whether a limitation on expression is constitutionally suspect must be assessed both by "the setting in which the speech occurs" and "on

45. European Commission Press Release, Implementing the European Agenda on Security—New Measures to Combat Terrorism and Illicit Trafficking of Firearms and Use of Explosives (Dec. 2, 2015), http://europa.eu/rapid/press-release_MEMO-15-6219_en.htm [https://perma.cc/VW8S-PJ2K].

46. This proposal is analogous to the requirement that social media companies report or provide means for users to report cyber terror to centralized law enforcement authorities. *See* Data Retention and Investigatory Powers Act 2014, c. 27, § 1 (UK), *amended by* Counter-Terrorism and Security Act 2015, c. 6, § 21 (UK); Bertrand Liard & Alexis Tandeau, *New French Act on Intelligence Services: Impacts on Technical Operators*, WHITE & CASE (Sept. 11, 2015), http://www.whitecase.com/publications/article/new-french-act-intelligence-services-impacts-technical-operators [https://perma.cc/B4MY-UX26].

47. R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) ("Content-based regulations are presumptively invalid.").

48. Holder v. Humanitarian Law Project, 561 U.S. 1, 25–39 (2010); Dennis v. United States, 341 U.S. 494, 516–17 (1951) (plurality opinion).

49. Miller v. California, 413 U.S. 15, 24 (1973).

50. Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942).

exactly what the speaker had to say."[51] First Amendment doctrine is not rigid; rather, it evolves through case-by-case developments. The specific words used and the context in which they are uttered are pertinent to First Amendment inquiry.

The internet is an evolving platform. It facilitates almost instant communications, but messages sent over it will rarely result in immediate breaches of the peace and, therefore, will ordinarily not involve fighting words.[52] Messages that might be dangerous in the context of face-to-face conflicts would more rarely have an immediate pugilistic effect when they are transmitted on the internet. That is not to say that the fighting-words doctrine is entirely irrelevant to cyberspace. Leaders of a terrorist organization can, for instance, use Twitter to direct immediate mayhem, as they did during the Mumbai attacks of 2008.[53] Terrorist propaganda often directs recipients to commit acts of violence at some unspecified time.[54] Moreover, insofar as some individuals may use social media to instigate immediate illegality, they and their accomplices would be personally culpable. The social media intermediary, as Part III explains, would likely claim to be civilly immune from liability for the fighting words posted by third parties.

A different barrier would confront litigants filing civil suits against social media companies, claiming to have suffered harms from allegedly threatening digital posts. To recover for true threats, a plaintiff must prove the defendant's culpability.[55] Under this doctrine, computer intermediaries are not culpable for acting as instruments for third parties, even when the latter intended the material to be threatening. Some websites and applications, however, are run by terrorist organizations and their minions, in which case the threat is directed by the web service.[56]

---

51. Young v. Am. Mini Theatres, Inc., 427 U.S. 50, 66 (1976) (footnote omitted). There are also essential ethical and social dimensions to the First Amendment that this Article only touches upon. *See generally* Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249 (1995); Alexander Tsesis, *Free Speech Constitutionalism*, 2015 U. ILL. L. REV. 1015; Alexander Tsesis, *Multifactoral Free Speech*, 110 NW. U. L. REV. 1017 (2016).

52. *Chaplinsky*, 315 U.S. at 572 (holding that fighting words "by their very utterance inflict injury or tend to incite an immediate breach of the peace" and are not protected by the First Amendment (footnote omitted)).

53. Jeremy Kahn, *Mumbai Terrorists Relied on New Technology for Attacks*, N.Y. TIMES (Dec. 8, 2008), http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html [https://perma.cc/7DS9-SKK5].

54. Eric Geller, *France Blames Facebook and Twitter for Terrorism*, DAILY DOT (Dec. 11, 2015, 9:45 AM), https://www.dailydot.com/layer8/france-social-networks-terrorism/ [https://perma.cc/8S8X-YTHE] (quoting the French secretary of state for European affairs as saying, "[i]n recent years, the Internet has become the major channel for terrorists to organize and to incite violent attacks"); Alroy Menezes, *Woman From Scotland Joined Islamic State to Become "Martyr,"* INT'L BUS. TIMES (Sept. 6, 2014, 10:21 AM), http://www.ibtimes.com/aqsa-mahmood-scotland-joined-islamic-state-become-martyr-1680588 [https://perma.cc/TG3X-FCBD] (reporting on a woman who allegedly used her Twitter account to encourage Muslims living in the West to perpetrate terrorist acts).

55. *See* Virginia v. Black, 538 U.S. 343, 366–67 (2003).

56. For a discussion of how terror groups rely on apps and encrypted software to communicate, see Robert Graham, *How Terrorists Use Encryption*, CTC SENTINEL, June 2016, at 20. For further discussion see Sean Gallagher, *ISIS Using Encrypted Apps for*

Unlike the fighting-words and true-threats doctrines, the material support of terrorism statute[57] offers an avenue of legal redress against internet information providers who refuse to take down terrorist content, especially when it leads to violence. The remainder of this Part discusses the general parameters of the material support doctrine, and Part III applies that doctrine to social media information providers.

In *Holder v. Humanitarian Law Project*,[58] the Supreme Court upheld a federal statute that prohibited persons and organizations from furnishing "material support or resources" to any group that the U.S. Department of State determined to be a foreign terrorist organization under the Immigration and Nationality Act.[59] The statute contains a scienter element, criminalizing only "knowingly" aiding[60] any group(s) practicing "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[61] The case was initially brought by Humanitarian Law Project, an organization that sought to counsel the Kurdish Workers' Party and the Liberation Tigers of Tamil Eelam, both on the designated terror list, about how to use international law, engage in politics, and lobby international organizations.[62]

The Court upheld the statute. Chief Justice Roberts, writing for the majority, made clear that when a party's statements are coordinated with a designated terrorist organization, the federal government has a compelling interest in public safety.[63] At the same time, simple advocacy of even heinous political perspectives are protected against government intrusions. The law did not prohibit individuals from proclaiming affinity for the banned groups, from adopting their political views, or even from associating with them.[64] The holding was in accord with erudite observations of Justices Robert Jackson and Arthur Goldberg that the Constitution is not a suicide pact.[65]

The First Amendment does not protect persons who or organizations that make statements on the internet advocating political violence, nor should it

---

Communications; Former Intel Officials Blame Snowden, ARS TECHNICA (Nov. 16, 2015, 4:46PM), https://arstechnica.com/information-technology/2015/11/isis-encrypted-communications-with-paris-attackers-french-officials-say/ [https://perma.cc/C8EG-DESE].

57. 18 U.S.C. § 2339B (2012).

58. 561 U.S. 1 (2010).

59. *Id.* at 39–40; *see also* 18 U.S.C. § 2339B(g)(6).

60. 18 U.S.C. § 2339B.

61. 22 U.S.C. § 2656f(d)(2) (2012).

62. *Humanitarian Law Project*, 561 U.S. at 14–15.

63. *Id.* at 40 ("The Preamble to the Constitution proclaims that the people of the United States ordained and established that charter of government in part to 'provide for the common defense.' . . . We hold that, in regulating the particular forms of support that plaintiffs seek to provide to foreign terrorist organizations, Congress has pursued that objective consistent with the limitations of the First and Fifth Amendments.").

64. *Id.* at 26.

65. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 159–60 (1963) (holding that the Fifth and Sixth Amendments applied to cases involving forfeiture of U.S. citizenship); Terminiello v. Chicago, 337 U.S. 1, 5, 37 (1949) (Jackson, J., dissenting) (dissenting from an opinion in which the majority held unconstitutional an ordinance that criminalized speech that "stirred people to anger, invited public dispute, or brought about a condition of unrest").

protect those who cooperated in the dissemination of foreign terrorists' materials. A disturbingly high number of parties spread and learn terrorism on the internet. Social media companies have provided them with the means of accessing recruits and coordinating with existing members. They rely on social media companies to disseminate their calls to arms. To avoid liability, it is logical to argue that Congress's compelling purpose to advance public safety includes demanding of persons aware they are disseminating foreign terrorists' messages to suspend or eliminate the materials.

It is one thing when virtually independent parties use Twitter accounts or Facebook pages to articulate offensive or noxious ideas and a very different matter when those who post are coordinating with organizations like ISIS, Hezbollah, Hamas, or Al Qaeda in an effort to invigorate and instruct persons to act on ideologically violent teachings. These are organizations that conspire with supporters to imperil innocents. When this activity becomes known to the digital intermediary, recalcitrant failure to take it down and report it to the proper law enforcement authorities entangles internet platforms with the terrorist activities.[66] Prohibiting internet information providers from knowingly publishing terrorist information and advocacy arises from "sensitive and weighty interests of national security and foreign affairs."[67] The compelling public interest in preventing mass casualties from terrorist attacks can be furthered by enforcing a narrowly tailored law against knowingly disseminating terrorist content through social media websites.

III. SOCIAL MEDIA LIABILITY

Enforcement of the material-support statute is likely to be the most efficient and effective way of combating terrorist incitement and recruitment on digital platforms. Social media companies have already taken some actions to combat online terrorist communications. For example, Facebook, Twitter, YouTube, and Microsoft established a jointly shared database of terrorist images.[68] This agreement will enable each company to be more aware of the digital materials that other platforms have identified to be extremist communications. While a positive step for diminishing terrorist influences on the internet, the method is woefully deficient because it does not require any of the platforms to take down offending images; indeed, each

66. This argument is informed, albeit not governed, by the Digital Millennium Copyright Act's safe harbor protection. *See* 17 U.S.C. § 512(c)(1)(A) (2012) (immunizing service providers from liability only if the service provider: "(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material"). While this statute deals with copyright violations, and is therefore not precisely on point with the material-support statute, the safe harbor's actual knowledge standard readily lends itself to digital material support for terror prosecutions.

67. *Humanitarian Law Project*, 561 U.S. at 33–34.

68. James Titcomb, *Facebook, Twitter and YouTube Create Database of Terrorist Images to Fight Online Extremism*, TELEGRAPH (Dec. 5, 2016, 11:01 PM), http://www.telegraph.co.uk/technology/2016/12/05/facebook-twitter-youtube-create-database-terrorist-images-fight/ [https://perma.cc/QP8K-UQN9].

of them has varying standards of community decency, and they might not even agree on what constitutes incitement, offense, or recruitment.[69] Federal law should create a uniform national mandate for public safety and security, rather than relying on corporate policies or disparate states' standards and law enforcement departments.

Pursuing litigation is strategically appropriate because social media providers have refused to take down many overtly terrorist posts on their own.[70] Ultimately, judges should protect constitutional rights of free speech, while recognizing congressional authority to enforce the Preamble of the Constitution's mandate to safeguard public safety.[71] Incitement published on U.S. social media poses significant dangers. Its impact is global. The French interior minister recently asserted that 90 percent of people who are recruited to terrorism are indoctrinated through internet content.[72]

Testimony before Congress in 2015 indicated that ISIS had over 46,000 Twitter accounts and that its followers sent between 90,000 and 200,000 tweets per day.[73] In addition, Twitter hashtags have included "#slaughter of Jews,"[74] and a Texas preschool teacher took to Twitter to insist on the need to "kill some Jews."[75] Other tweets encourage violence: "Kill jews. Kill all of them," "Happy international stab a Jew day," and "Stab Jews and have a juice."[76] Among the many other tweets calling for violence were those of a Syrian jihadist under his own name, Abu Khalid al-Amriki, "We love death

---

69. *Id.*

70. *See supra* Part I.

71. U.S. CONST. pmbl. The Supreme Court has recognized that the Preamble to the Constitution contains a national mandate to secure the public defense. *Humanitarian Law Project*, 561 U.S. at 40.

72. Frédéric Donck, *Digital Single Market*, ISOC EUR. REGIONAL BUREAU NEWSL. (Internet Soc'y, Geneva, Switz.), Feb. 23, 2015, at 3.

73. *ISIL in America: Domestic Terror and Radicalization: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 114th Cong. 3 (Feb. 26, 2015) (asserting that there are 90,000 ISIS-related tweets per day); 161 CONG. REC. H9316 (daily ed. Dec. 15, 2015) (statement of Rep. Ros-Lehtinen) (asserting that there are 200,000 ISIS-related tweets per day); J.M. Berger, *Can We Win the War Against ISIS by Focusing on Social Media?*, HUFFINGTON POST, http://www.huffingtonpost.com/jm-berger/isis-social-media_b_6733206.html [https://perma.cc/4VP9-YCQH] (last visited Oct. 16, 2017).

74. Eliezer Sherman, *Report: Palestinian Stabbing Attacks Inspiring ISIS Supporters to Offer Guidance*, ALGEMEINER (Oct. 14, 2015, 1:13 PM), https://www.algemeiner.com/2015/10/14/report-palestinian-stabbing-attacks-inspiring-isis-supporters-to-offer-guidance/ [https://perma.cc/BUR4-BAJ4]; *Slaughter the Jew*, DIGITAL TERRORISM & HATE 2017, http://digitalhate.net/inicio.php [https://perma.cc/MB6D-DW7Y] (search the search field for "slaughter the Jew").

75. *'Kill Some Jews' Tweet Gets Texas Pre-School Teacher Fired*, FOX NEWS (Feb. 22, 2017), http://www.foxnews.com/us/2017/02/22/kill-some-jews-tweet-gets-texas-pre-school-teacher-suspended.html [https://perma.cc/E38U-4HFB]. The teacher seems to have disabled her own Twitter account after the news media exposed her post. Lea Speyer, *Texas Pre-School Teacher Removed from Classroom After Twitter Calls to 'Kill Some Jews' Comes to Light*, ALGEMEINER (Feb. 21, 2017, 3:59 PM), https://www.algemeiner.com/2017/02/21/texas-pre-school-teacher-removed-from-classroom-after-twitter-calls-to-kill-some-jews-come-to-light/ [https://perma.cc/5A9P-X5EU].

76. Anti-Defamation League, *Incitement to Violence Against Jews Spreads Online*, ADL BLOG (Oct. 9, 2015), https://www.adl.org/blog/incitement-to-violence-against-jews-spreads-online [https://perma.cc/KX25-N9RW].

more than you love life. We love Prophet Muhammad . . . more than we love our own selves. Kill those that insult the Prophet."[77] Using another Twitter account, Jihadi John, an infamous ISIS executioner, tweeted admonitions to emulate previous terrorist attackers like Mohamed Atta (the leading figure of the World Trade Center attacks on September 11, 2001) as well as Dzhokhar and Tamerlan Tsarnaev (the Boston Marathon bombers).[78] These were overtly violent and inciteful. Investing more to improve algorithmic software, developed to classify syntactic and semantic strings of violent terrorist messages, could have enabled Twitter to quickly eliminate these hostile expressions.[79]

Federal enforcement of the material-support statute against social media organizations is likely to incentivize them to allocate additional capital to develop software that, at a minimum, can detect overtly violent incitement. But the public's need for national security must be balanced against legitimate concerns for personal autonomy and privacy. The information, coupled with data collection, unmasks IP addresses of designated terror organizations and uses fingerprinting technologies to recognize the pictorial pixels of previously identified terrorist organizations' digital imagery.[80] Such information will facilitate social media vigilance, but to avoid violations of civil liberties, law should provide for (1) proprietary data security; (2) procedural transparency into investigations, except in matters of national emergency, allowing social media companies to challenge government demands for information; and (3) procedural safeguards both for ongoing and emergency investigations. Critical to the protection of privacy is the enforcement of an independent judicial authority to review law enforcement demands for customer data.

In addition to Twitter, ISIS and other designated terrorist organizations rely on a variety of other digital platforms, including Facebook, Kik, WhatsApp, YouTube, and Ask.FM.[81] YouTube is one of the most effective tools for terrorist recruitment.

---

77. Daniel Greenfield, *ISIS Jihadists Threaten Frontpage Mag*, FRONTPAGE MAG (May 4, 2015), http://www.frontpagemag.com/point/256365/isis-jihadists-threaten-frontpagemag-daniel-greenfield [https://perma.cc/J5P4-7PYK].

78. Jihadi John, DIGITAL TERRORISM & HATE 2017, http://digitalhate.net/inicio.php# [https://perma.cc/MB6D-DW7Y] (search the search field for "jihadi john").

79. Scholars have performed several studies on data mining and algorithmic frameworks for identifying terrorist and otherwise hostile messaging on social media. *See generally* Pete Burnap & Matthew L. Williams, *Cyber Hate Speech on Twitter: An Application of Machine Classification and Statistical Modeling for Policy and Decision Making*, 7 POL'Y & INTERNET 223 (2015); Marc Cheong & Vincent C. S. Lee, *A Microblogging-Based Approach to Terrorism Informatics: Exploring and Chronicling Civilian Sentiment and Response to Terrorism Events via Twitter*, 13 INFO. SYSTEMS FRONTIERS 45 (2011); Ellen Spertus, *Smokey: Automatic Recognition of Hostile Messages*, 1997 IAAI PROC. 1058.

80. Adam Tanner, *The Web Cookie Is Dying. Here's the Creepier Technology That Comes Next*, FORBES (June 17, 2013, 12:29 PM), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/ [https://perma.cc/62F6-FZ2F].

81. ANTI-DEFAMATION LEAGUE, RESPONDING TO CYBERHATE: PROGRESS AND TRENDS 9–10 (2016).

A video that has since been removed from YouTube spelled out "44 way [sic] to support jihad Shaikh Tamim Al Adnani," and contained gruesome imagery with a running ticker encouraging viewers to send financial contributions, disseminate jihad, engage in arms training, and translate jihadi literature.[82] As on other social media websites, Facebook accounts that advocate on behalf of terrorists are sometimes briefly removed only to reappear again under a different moniker, as was the case with Abu Haleema's account, which advocated for violence and intolerance.[83] Facebook likewise took down Hamas's glorifications of a terrorist bomb-maker but, for a time, left untouched a Palestinian authority's Facebook lionization of the same "engineer" and its exhortation calling on others to follow his martyrdom.[84]

While social media companies have independently worked to eliminate many terrorist postings, they are too often recalcitrant, tardy, or uncooperative in responding to law enforcement agencies' or public watchdogs' requests for removal of designated terrorists' web postings.[85] To date, the federal government has been hesitant to enforce the material-support statute against social media companies. The Constitution limits the power of government to intrude on these companies' speech rights to eschew the official censorship of debates, even when they involve obnoxious and offensive statements. The First Amendment even protects expressions of violent political philosophy or religious doctrine.[86] Individual liability arises when a party issues a true threat[87] or cooperates with a foreign terrorist organization.[88] Social content providers have no legal obligation to remove abstract statements that favor terrorist groups but neither advocate violence against anyone nor support terrorist organizers.[89] However, a social media

82. This video was previously available at Mohd Zhukrie bin Nawang, *44 Way to Support Jihad Shaikh Tamim Al Adnani*, YOUTUBE (July 22, 2013), https://www.youtube.com/watch?v=Gml2q-6n_Lc [https://perma.cc/M5BT-UZKH] (last visited Aug. 4, 2017).

83. Daniel Peters et al., *Extremist London Preacher Who 'Giggled' at an ISIS Beheading Video Is Gaining an Australian Following After Posting YouTube Videos Attacking Moderate Sydney Sheikhs*, DAILY MAIL (Jan. 20, 2016, 11:49 AM), http://www.dailymail.co.uk/news/article-3408512/Abu-Haleema-gaining-following-Australians-posting-YouTube-videos-attacking-moderate-Sydney-sheikhs.html [https://perma.cc/8VUH-A5KK].

84. Dov Lieber, *Facebook Closes over 100 Hamas-Linked Accounts, Angering Terror Group*, TIMES ISR. (Jan. 8, 2017), http://www.timesofisrael.com/facebook-closes-over-100-hamas-linked-accounts-angering-terror-group/ [https://perma.cc/ZD6S-VHAG].

85. *See Are Social Media Companies Doing Enough to Combat Internet Extremism?*, JAN Trust (Feb. 16, 2016), https://jantrust.wordpress.com/2016/02/16/are-social-media-companies-doing-enough-to-combat-internet-extremism/ [https://perma.cc/P95Z-CLDR].

86. *See* Scales v. United States, 367 U.S. 203, 229 (1961) ("[The Free Speech Clause] does not make criminal all association with an organization which has been shown to engage in illegal advocacy. There must be clear proof that a defendant 'specifically intend[s] to accomplish [the aims of the organization] by resort to violence.'" (quoting Noto v. United States, 367 U.S. 290, 299 (1961))).

87. *See* Virginia v. Black, 538 U.S. 343, 359–60 (2003).

88. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 36–38 (2010).

89. *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam). Indeed, several terrorist social media sites are purportedly used by national intelligence organizations for clandestine espionage. *See* Roi Kais, *Hezbollah's Battle Against Mysterious 'Zionist'*

company that is made aware that a foreign terrorist organization has uploaded materials on its platform should be legally obligated to remove it, report it to law enforcement authorities, and share the information with other internet information providers. They also should be held criminally liable to communicate the gravity of helping terrorists advance their machinations.

The companies will want to keep proprietary information confidential, but profit motive and corporate efficiency are not important enough interests to gainsay the compelling government interest to enforce laws narrowly tailored to secure public safety. There is no First Amendment right to be a venue for terrorist propaganda, indoctrination, threats, recruitment videos, or weapons-making instructions. Communications platforms, such as YouTube, should enjoy no immunity for knowingly hosting operational contents for groups bent on mass murder and havoc such as Al Qaeda or ISIS.

True threats and material support of terrorist organizations are unprotected forms of speech because they raise grave safety concerns. In circumstances where the internet information provider is unaware of the posting, it cannot be held accountable. However, where it is made aware by law enforcement agents or private citizens, the entity is on notice that indifference, intransigence, or other lack of effort to investigate and take down the offending material can subject it to criminal liability. Under those circumstances, a social media provider should be required to take affirmative steps both to remove the offending materials and to develop software designed to prevent terrorist organizations from reappearing under different accounts. Identifying the initiators of the postings can be done through simple ISP identification, which tracks the activities of a specific computer account, and through sophisticated, semantic algorithms or fingerprinting technologies.

A. Civil Liability

A party seeking to establish civil liability against a social media outlet would face an uphill battle. The outcome of private litigation, filed pursuant to the civil remedy provision of the Anti-Terrorism Act,[90] is far from certain. This avenue of redress nevertheless warrants analysis.

A civil lawsuit might be brought against a social media company that knowingly cooperates with designated foreign terrorists in posting, displaying, or housing propaganda.[91] Scienter may be satisfied when an entity recognizes it is supporting a terrorist organization; it need not be aware that its aid is going to advance a specific terrorist conspiracy.[92] Secondary liability against entities operating in the United States would increase the

Campaign, YNETNEWS.COM (Apr. 13, 2017, 1:27 PM), http://www.ynetnews.com/articles/0,7340,L-4948783,00.html [https://perma.cc/E4C8-WG8Q].

90. 18 U.S.C. § 2333 (2012).

91. *Cf.* Boim v. Quranic Literacy Inst. & Holy Land Found. for Relief & Dev., 291 F.3d 1000, 1028 (7th Cir. 2002) (holding that secondary liability is available under the Anti-Terrorism Act for knowing financial support of foreign terrorist organizations).

92. *Humanitarian Law Project*, 561 U.S. at 16–18.

likelihood of collecting judgments, since many terrorists and their sources of capital are outside the country.[93]

Mainstream social media companies do not create terrorist statements. However, the companies often allow terrorists and terrorist organizations to use their platforms for disseminating terrorist propaganda. Taking a purely textualist approach to statutory interpretation, the language of the statute appears to permit victims of terrorism or their survivors to file lawsuits against social media companies only in a narrow set of circumstances.[94] The statute specifically permits suits to be brought against a person or entity that allegedly "aids and abets, by knowingly providing substantial assistance" to a "person who committed such an act of international terrorism."[95] Under this statutory provision, liability could only be found if the digital information company "authorized" the designated terrorist organization to commit, plan, or provide substantial assistance to international terrorist organizations to commit those acts.[96] Arguably, knowing authorization may include granting a designated terrorist organization the right to maintain a digital social media account.

The statute does not countenance courts, legislators, or administrators subjectively deciding what association qualifies as a terrorist organization. The Immigration and Nationality Act does not leave the definition of a terrorist organization ambiguous;[97] rather, it requires the Department of State to engage in nonarbitrary administrative hearings before designating an association a foreign terrorist organization.[98] Terrorist organizations engage in atrocities, such as hijacking vehicles; seizing and detaining persons; "threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained"; engaging in assassination; using biological, chemical, or nuclear agents; and similarly egregious misconduct.[99]

Despite the availability of treble damages under the Anti-Terrorism Act,[100] there is a significant hurdle to success in seeking to hold social media information companies accountable. Since 1997, federal courts have developed a doctrine of immunity that protects computer content disseminators from civil liability. The pertinent statute, § 230 of the CDA, grants immunity to "provider[s] or user[s] of an interactive computer service" from being held responsible for content created by a third party.[101] Courts have extended application of this language to digital information distributors even when they have notice and have been made aware that they are hosting

93. Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 690 (7th Cir. 2008).
94. 18 U.S.C.A. § 2333(a) (Westlaw 2016).
95. *Id.* § 2333(d)(2).
96. *Id.*
97. 8 U.S.C. § 1189 (2012).
98. *Id.* § 1189(c).
99. *Id.* § 1182(a)(3)(B)(iii).
100. 18 U.S.C.A. § 2333(a).
101. 47 U.S.C. § 230(c)(2) (2012).

defamatory content on their internet platforms.[102] Courts have interpreted § 230 to apply to internet intermediaries that host third-party content. There is a general consensus among judges that Congress intended digital platforms to be immune, expecting thereby to promote a robust market for free speech and to sanction internet intermediaries to selectively police websites for offensive content.[103] The law passed in response to a state court's holding that internet companies were subject to defamation suits simply for exercising editorial control.[104] With the passage of § 230(c)(2), Congress undertook to protect internet information providers who in good faith screen, remove, or block materials they believe to be "excessively violent . . . or otherwise objectionable."[105] The judicial consensus holds that, subsequent to the enactment of § 230, information service companies can no longer be held accountable when they function as neutral conduits for information or selectively remove content.[106]

Circuit courts throughout the country have deferred to Congress's reliance on corporate responsibility to uphold the rationale for § 230 immunity,[107] which they believe incentivizes companies like Yahoo!, Twitter, and Facebook to take independent actions to monitor their services to prevent the posting and retention of terrorist messages. However, there is reason to doubt this accepted interpretation of § 230. Some scholars have argued that these internet information providers are distributors that do not qualify for § 230 publisher immunity.[108] Because social media companies are more involved

---

102. Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) (recognizing § 230 immunity on the basis of a "well established" judicial rule "that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech"); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 331–34 (4th Cir. 1997).

103. The statute creates the following treatment of any "publisher or speaker": "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." 47 U.S.C. § 230(c)(1); *see also Zeran*, 129 F.3d at 330 (interpreting § 230); Benjamin C. Zipursky, *Thinking in the Box in Legal Scholarship: The Good Samaritan and Internet Libel*, 66 J. LEGAL ED. 55, 59–60 (2016) (discussing statutory interpretation of § 230).

104. Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063-94, 1995 WL 323710, at *6 (N.Y. Sup. Ct. May 24, 1995).

105. *Zeran*, 129 F.3d at 331 ("Congress enacted § 230 to remove the disincentives to selfregulation created by the *Stratton Oakmont* decision."). Section 230(c)(2)(A) reads:

> No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

47 U.S.C. § 230(c)(2)(A).

106. *See, e.g.*, Klayman v. Zuckerberg, 753 F.3d 1354, 1358 (D.C. Cir. 2014); FTC v. Accusearch Inc., 570 F.3d 1187, 1199–1200 (10th Cir. 2009); Jurin v. Google Inc., 695 F. Supp. 2d 1117, 1122–23 (E.D. Cal. 2010); Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1197–98 (N.D. Cal. 2009).

107. *See* Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003); Green v. Am. Online, Inc., 318 F.3d 465, 470 (3d Cir. 2003); Ben Ezra, Weinstein, & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).

108. Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 637–42 (2001); Sewali K. Patel, Note, *Immunizing Internet Service Providers from Third-Party Internet Defamation*

in the selection of disseminated information than traditional publishers, they do not qualify for the CDA's immunity provision.[109]

Once the internet information company is informed that there is illegal content on its websites—such as material support of terror—it no longer functions simply as a passive conduit for information. Indeed, the extent of immunity has been severally parsed by differing federal courts of appeals. An early case, *Zeran v. America Online, Inc.*,[110] held that § 230 creates blanket immunity from liability.[111] However, a more recent case from a different federal circuit, *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*,[112] questioned the court's finding in *Zeran* of "broad immunity from liability for unlawful third-party content."[113] In *Chicago Lawyers'*, the court pointed out that internet information providers are not immune from liability arising from participation or encouragement of illegal activity, such as copyright infringement.[114] One can extrapolate from the latter holding that any computer service engaged in terrorist recruitment would not be protected under § 230. But this has no application to Twitter, Google, and Facebook, which post no terrorist materials of their own. Indeed, they eliminate many third-party posts containing such content. Nevertheless, those companies have not done enough to mitigate damages from terrorists who exploit their services to incite and propagandize.[115] For the time being, § 230 immunity is deeply entrenched in most circuits that have addressed the topic. The law is unlikely to change without congressional revision of the statute.

That is not, however, to say that civil liability is entirely precluded. Benjamin Wittes and Zoe Bedell proffer a suggestion that even taking for granted civil immunity in ordinary tort cases, social media companies that violate the material-support statute should not be similarly immune.[116] They argue that social information websites, such as Twitter, that host terrorists' posts are not immune from liability because § 230(e)(1) contains an exception: "Nothing in this section shall be construed to impair the

---

Claims: How Far Should Courts Go?, 55 VAND. L. REV. 647, 651–53 (2002). The Center for Law and Information Policy at Fordham University School of Law has compiled an excellent synopsis of articles criticizing or defending § 230 immunity. JOEL R. REIDENBERG ET AL., CTR. ON L. & INFO. POLICY, SECTION 230 OF THE COMMUNICATIONS DECENCY ACT: A SURVEY OF THE LEGAL LITERATURE AND REFORM PROPOSALS 22–35 (2012).

109. Patel, *supra* note 108, at 680–83.

110. 129 F.3d 327 (4th Cir. 1997).

111. *Id.* at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."); *see also* Glob. Royalties, Ltd. v. Xcentric Ventures, LLC, 544 F. Supp. 2d 929, 932 (D. Ariz. 2008) ("[T]he CDA is a complete bar to suit against a website operator for its 'exercise of a publisher's traditional editorial functions.'" (quoting *Zeran*, 129 F.3d at 330)).

112. 519 F.3d 666 (7th Cir. 2008).

113. *Id.* at 669.

114. *Id.* at 670.

115. *See supra* Part I.

116. *See* Benjamin Wittes & Zoe Bedell, *Did Congress Immunize Twitter Against Lawsuits for Supporting ISIS?*, LAWFARE (Jan. 22, 2016, 9:14 AM), https://www.lawfareblog.com/did-congress-immunize-twitter-against-lawsuits-supporting-isis [https://perma.cc/Y97D-6XVP].

enforcement of . . . any . . . Federal criminal statute."[117] Wittes and Bedell's insightful observation does not, however, fully resolve the matter because it is likely that a digital media platform would claim immunity by arguing that it had not engaged in material support of terrorist organizations, even when it carries terrorist content that a third party created and posted on its platform. In anticipation of this defense, complainants would significantly increase their chances of success by delaying the filing of a civil suit until after the prospective defendant's criminal conviction for material support.[118] Put in more technical terms, civil material-support litigation[119] should follow on the heels of criminal material-support conviction.[120]

A civil litigant would also need to prove causation. A proper party plaintiff would need to demonstrate that he or she suffered harm that was actually and proximately caused by the digital information provider's material support of a foreign terrorist organization.[121] In addition to proving that a company knew it was profiting from hosting the violent entity on its platform, a complainant would need to demonstrate that the posted material advanced a designated terrorist organization's agenda.[122] Litigants would need to gather evidence demonstrating that they suffered actual harm from the internet information service's decision to ignore complaints about the posting of foreign terrorist materials on its website.[123]

The case could be built on evidence that would include a record of complaints the company had received about specific webpages, videos, posts, articles, IP addresses, or accounts of foreign terrorist organizations; the company's failure to remove the material; a terrorist's subsequent viewing of or interacting with the material on the website; and that terrorist's acting upon the propaganda to harm the plaintiff. Such a lawsuit likely would be difficult to win, but success would not be precluded because § 230(e)(1) provides that information providers are not exempt from culpability for criminal activity, including the material support of terrorism.[124]

Given the current judicial trend finding digital information intermediaries to enjoy civil immunity, Congress should consider advancing new legislation to clarify that § 230 does not apply to litigation seeking a remedy against data that are materially supportive of foreign terrorist organizations. The terms of immunity so tie the hands of litigants that some modification of the statute is in order. The safe harbor provision might be reenacted to include a provision

117. *Id.*

118. *See* Hinton v. Amazon.com.dedc, LLC, 72 F. Supp. 3d 685, 691 (S.D. Miss. 2014) (citing and agreeing with a variety of federal courts that found that mere allegations of criminality included in a civil suit do not negate § 230(c) immunity).

119. 18 U.S.C. § 2333 (2012).

120. 18 U.S.C. § 2339B (2012).

121. *See* Beyond Sys., Inc. v. Kraft Foods, Inc., 777 F.3d 712, 716, 718 (4th Cir. 2015) (finding standing where an internet service provider consented to the alleged legal harm).

122. *See* Benjamin Wittes, *Another Day, Another Material Support Suit Against a Social Media Company*, LAWFARE (Jan. 10, 2017, 4:55 PM), https://www.lawfareblog.com/another-day-another-material-support-suit-against-social-media-company [https://perma.cc/D52M-DATN].

123. *See Beyond Sys.*, 777 F.3d at 716.

124. 47 U.S.C. § 230(e)(1) (2012).

that explicitly excludes from coverage organizations and individuals who pose national security risks. That does not get around the need to prove causation; therefore, the likelihood of success at the motion to dismiss, summary judgment, or merits phases of litigation remains small. However, where Twitter, Facebook, YouTube, and similar content carriers receive notice of terrorist statements that harmed or are likely to result in attacks against a party, a court should find standing for a plaintiff to proceed with a civil suit for compensatory, injunctive, or punitive relief.

B. Criminal Liability

Social media services have expanded the expressive reach of terrorists by providing them with outlets for mobilizing individual attacks by "lone wolves," many of whose first contacts with these organizations were through the internet.[125] Civil remedies are difficult to obtain against social media companies.[126] A strategy more likely to succeed would be for the Justice Department to file criminal complaints against companies for violating the true-threats statute[127] or material-support statute.[128] Criminal liability could include monetary fines, orders for internet information providers to maintain records of IP addresses and contents found on foreign terrorist webpages, and takedown orders. In addition, culpable companies could be enjoined to create hyperlinks on suspect pages, enabling users to directly inform appropriate national intelligence agencies of suspicious materials.

Administrative agencies, to be on the front lines of fair and thorough investigations, will also need to promulgate new regulations. The terms of regulation should be attentive to the doctrinal balance between the often conflicting compelling interests of national security and free expression. This will require enforcement of narrowly tailored rules that will not limit more speech than necessary for national security. These regulations should be passed only after extensive hearings and studies about effective methods of enforcing the material-support law against recalcitrant social media companies. The public agency in charge of the program will need investigative powers to gather pertinent data. Mechanisms will also need to be created that can enable administrators to take emergency measures, while simultaneously preserving the due process rights of internet intermediaries to challenge orders to immediately block, temporarily remove, or permanently destroy data.

Relying on the material-support statute or true-threats statutes could effectively prevent abusive government censorship. Of course, there is a risk of law enforcement overreaching, but the same can be said about almost any

125. *Terrorism in Africa: The Imminent Threat to the United States: Prepared Testimony Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec.*, 114th Cong. 3, 7 (2015) (statement of Daniel Byman, Director of Research, Center for Middle East Policy, Brookings Institute), https://homeland.house.gov/hearing/subcommittee-hearing-terrorism-africa-imminent-threat-united-states/ [https://perma.cc/PSE2-H7LS].

126. *See supra* Part III.A.

127. 18 U.S.C. § 875(c) (2012).

128. 18 U.S.C. § 2339B(a) (2012).

criminal law. Nevertheless, social media organizations cannot be held accountable for anything a private complainant or law enforcement agency regards to be offensive. Criminal charges can be brought when an internet information provider refuses to comply with a federal agency request to take down the threatening or inciteful content that a designated terrorist organization placed on its server. They can also be brought for failure to remove direct and intentional targeting of threats against individuals. If any charges are filed, a party must be afforded notice, an opportunity to be heard, and judicial relief against arbitrary state encroachment on the company's legitimate speech interests.

Some litigation will no doubt involve evidence directly impacting national security. In those circumstances, government should nevertheless provide a defendant with adequate access to documentation, affidavits, and physical objects to mount a defense. An in camera hearing might be required for the government to divulge particularly sensitive information to a judge, in which case, the defense attorney would need to have an appropriate level of security clearance.[129] Furthermore, because speech is of such importance to deliberative democracy, requiring plaintiffs to pay attorneys costs to social media companies that mount successful challenges would be a deterrent against groundless litigation.

In addition to takedown orders against terrorist digital accounts—which might later crop up under new hashtags, html addresses, or profiles—a court might also issue an injunction to develop or deploy algorithmic software for identifying offending sites used to overtly incite audiences to commit acts of violence or to provide material support in the recruitment or operationalization of terror.[130] This mechanical fix would diminish, though it would not entirely eliminate, the sheer number of terrorist materials that are regularly transmitted through websites like Twitter.

Currently, ISIS and other terrorist organizations rely extensively on Twitter.[131] The company only selectively culls terroristic texts, in part because its employees may not be able to distinguish between the promotion of terrorism and political advocacy.[132] Terrorists exploit the company's liberality. Twitter remains a platform for propagandizing, inciting, and

129. *See* Margaret B. Kwoka, *The Procedural Exceptionalism of National Security Secrecy*, 97 B.U. L. REV. 103, 108, 135–36 (2017).

130. Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, http://lthoumyre.chez.com/txt/jurisfr/cti/yauctions20000522.htm [https://perma.cc/6QAP-DQZB] (UEJF & LICRA v. Yahoo! Inc. & Yahoo France); *see also* Marc H. Greenberg, *A Return to Lilliput: The* LICRA v. Yahoo! *Case and the Regulation of Online Content in the World Market*, 18 BERKELEY TECH. L.J. 1191, 1209–10 (2003) (citing the French court's order that Yahoo! develop software capable of identifying illegal sales of Nazi paraphernalia through its French website). While the company initially claimed it could not effectively comply with the order, it soon began to block the offending materials from being accessible through its French search engine. Orin S. Kerr, *Enforcing Law Online*, 74 U. CHI. L. REV. 745, 746–47 (2007).

131. *See* Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015), https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ [https://perma.cc/G6BA-4MK3].

132. *See id.*

spreading operational instructions.[133] Terrorists exploit U.S. companies' seeming naiveté about the ability of terrorists to advance their recruitment and violent objectives by communicating through digital networks. Where there is a compelling state interest in public safety, courts should be granted authority to issue warrants requiring companies to reveal identifying information concerning foreign terrorists' accounts.

The Supreme Court has set several significant barriers to prevent the government from abusing the material-support statute for arbitrary censorship. One such barrier is judicial review. In *Humanitarian Law Project*, the Court held that Congress has the authority to rely on expert evidence to identify "particularly dangerous and lawless foreign organizations."[134] The secretary of state can only place a group on the list of designated terrorist organizations after extensive evidence gathering reveals the group to have a history of ideologically driven violent activities, such as killings and bombings.[135] Federal law also requires the Department of State to evaluate whether designating an entity a terrorist association will have consequences on "national defense, foreign relations, or economic interests."[136]

Furthermore, the secretary must notify suspected groups and offer them opportunities to rebut findings, with the caveat that they will have only limited access to classified documents.[137] The law thereby creates "stringent requirements" for designating a group a foreign terrorist organization.[138] The First Amendment should not protect social media information providers who materially support groups that, after extensive intelligence gathering and opportunity to be heard, were designated as foreign terror organizations. To date, social media organizations provide designated terrorist entities with platforms for propaganda, indoctrination, and recruitment materials that influence susceptible persons to engage in violent and ideological schemes.

However post hoc complaints would fare, it is clear that the government is prohibited from imposing prior restraints on speech, except in cases of national emergency.[139] This is especially the case when the government relies on an act of Congress, such as the material-support or true-threats statutes, to advance national security interests.[140] In the case of a pressing and clearly defined national emergency, narrowly tailored restrictions prior to publication may be constitutionally permissible.

---

133. *Id.*
134. Holder v. Humanitarian Law Project, 561 U.S. 1, 40 (2010).
135. People's Mojahedin Org. of Iran v. U.S. Dep't of State, 182 F.3d 17, 24–25 (D.C. Cir. 1999).
136. 8 U.S.C. § 1189(a)(1)(C), (d)(2) (2012).
137. Nat'l Council of Resistance of Iran v. Dep't of State, 251 F.3d 192, 208–09 (D.C. Cir. 2001).
138. Boim v. Quranic Literacy Inst. & Holy Land Found. for Relief & Dev., 291 F.3d 1000, 1027 (7th Cir. 2002).
139. Near v. Minnesota, 283 U.S. 697, 716 (1931).
140. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 718–19 (1971) (Black, J., concurring).

To effectuate its investigation, the government may issue national security letters (NSLs) to identify terrorists' IP addresses and similar information known only to the internet information companies. NSLs do not require prior judicial proceedings and can be kept confidential throughout the investigation.[141] Companies unwilling to comply are granted the right of judicial review.[142]

It is important to stress that there is a strong presumption against prior restraints on speech; therefore, except in rare cases of immediate national emergencies,[143] the government should only pursue internet service companies that have intentionally cooperated with a designated terrorist organization to upload or maintain digital accounts. Indeed, the NSL system has a variety of components that raise some serious concerns, including a lack of constitutional protections prior to the initiation of an investigation and lack of public oversight. This Article has, however, focused on the cases where investigators only need to use ordinary searches, rather than intrusive surveillance, to investigate and file charges requesting takedown orders, injunctions, and damages. Criminal law should focus on publicly available digital materials and therefore existing expressive conduct, which raises no prior restraint issues.

C. International Guidelines

In drafting a material-support statute providing specific due process rights and remedies in material-support criminal actions brought against social media intermediaries, Congress should not act in a vacuum. Rather, it should look to international legislative models. Canada is an example of an open and vibrant democracy that empowers courts to order removal of electronic copies of hate propaganda that are maintained on computer systems located within the country's jurisdiction.[144] The Canadian criminal code grants judges the power to

> order the custodian of the computer system to (a) give an electronic copy of the material to the court; (b) ensure that the material is no longer stored on and made available through the computer system; and (c) provide the information necessary to identify and locate the person who posted the material.[145]

Like the United States, Canada places great emphasis on the importance of free speech to a democracy. Nevertheless, restrictions on hate speech, such as the online support of terrorism, go hand-in-hand with the nation's guarantee of free expression in the Canadian Charter of Rights and Freedoms.

---

141. 18 U.S.C. § 2709(a)–(c) (2012).

142. *Id.* § 2709(d).

143. Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976); Carroll v. President & Comm'rs of Princess Anne, 393 U.S. 175, 181 (1968).

144. Canada Criminal Code, R.S.C. 1985, c C-46, § 320.1; *see also About the Anti-terrorism Act*, CAN. DEP'T JUST. (July 26, 2017), http://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html [https://perma.cc/H5EV-ENM7] (explaining section 320.1).

145. Canada Criminal Code, R.S.C. 1985, c C-46, § 320.1.

The country's supreme court recognizes three principal values associated with the constitutional guarantee of free expression: the quest for truth, the pursuit of "social and political decision-making," and the individual's desire to enjoy "self-fulfillment and human flourishing."[146] Canada does not, however, maintain a libertarian regime; it instead acknowledges that "reasonable limits prescribed by law" are conducive for safeguarding "a free and democratic society."[147] The centrality of free speech to Canadian pluralistic society does not countenance the electronic dissemination of terrorist materials through computer systems.[148]

The Canadian Anti-Terrorism Act grants courts additional power to identify terrorist propaganda on computer systems that are available to the public.[149] Judges can order a "computer system's custodian to delete the material."[150] Prior to the deletion, a court must provide notice and an opportunity to be heard in court to the party who posted the materials. Or, if that party cannot be located or is outside Canada, a judge can order the computer system's custodian to post a notice of removal in the digital space where the document had previously been available.[151]

Materials containing hate propaganda are unprotected.[152] Canada clearly distinguishes constitutionally protected free speech from terrorist and hate propaganda. Terrorist ideology is not a form of deliberation but a strategic means of recruitment, organization, planning, misinformation, antagonism, and threat.[153] Nor does Canada recognize the promotion of terrorism to be protected by its constitutional guarantee of free association.[154]

A digital intermediary is unlikely to be liable for "innocent dissemination" of terrorist information. This Article extrapolates this premise from Canadian defamation law, which exonerates a party who facilitates the circulation of false and harmful information without "actual knowledge" of

146. Regina v. Keegstra, [1990] 3 S.C.R. 697, 728 (Can.).

147. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11 (U.K.).

148. COMPUTER SECURITY HANDBOOK § 72.1.3.2 (Seymour Bosworth et al. eds., 6th ed. 2014) ("Canadian law directs courts to balance an individual's free speech rights with societal equality interests. Thus, Canadian courts have upheld hate speech convictions under laws that criminalize the willful promotion of hatred.").

149. Anti-terrorism Act, S.C. 2015, c 20, § 35 (Can.).

150. *Id.*

151. Anti-terrorism Act, S.C. 2001, c 41, § 320.1(2) (Can.).

152. *Id.*

153. *Cf.* Regina v. Khawaja, [2012] 3 S.C.R. 555, 585 (Can.) ("This Court's jurisprudence supports the proposition that the exclusion of violence from the s. 2 (b) [of the Canadian Charter] guarantee of free expression extends to threats of violence. . . . As this Court held in *Greater Vancouver Transportation Authority*, 'violent expression *or threats of violence* fall outside the scope of the s. 2 (b) guarantee.' It makes little sense to exclude acts of violence from the ambit of s. 2 (b), but to confer protection on threats of violence." (quoting Greater Vancouver Transportation Authority v. Canadian Federation of Students—British Columbia Component, [2009] 2 S.C.R. 295, para. 28 (Can.))); Ahani v. Canada, 2000 CarswellNat 74, para. 18 (Can. Fed. Ct.) (WL).

154. Canada v. I.L.W.U., Local 500, 2009 CarswellNat 3151, 2009 CarswellNat 5796 (Can. Fed. Ct. of App.) (WL) ("[S]ection 2 [of the Charter] does not protect the freedom to associate in order to engage in or promote violent, terrorist or other criminal activities.").

the content.[155] Using this analogous model of liability, a social media company might argue in defense that it had "no actual knowledge" that would put it "on notice to suspect" the existence of terrorist incitement on its server.[156] Speech is of such great constitutional importance that computer intermediaries are likely protected against liability for unknowingly and unintentionally hosting terrorist hyperlinks and other materials posted by third parties.

The European Union has likewise recognized the dangers of terrorist groups' propaganda on social media. The EU's official statement warns that terrorist organizations exploit social media to recruit, radicalize, and instruct their supporters.[157] The European Convention on the Prevention of Terrorism requires the forty-seven member states of the Council of Europe to criminalize the "public provocation to commit a terrorist offence."[158] The Convention prohibits the "distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offense, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed."[159]

Article 5 of the Convention is consistent with the U.S. material-support doctrine as both criminalize only intentional utterances that are directed at the public.[160] This is not to say that Article 5 is entirely consistent with U.S. free speech doctrine. In addition to true threats, the Convention also obligates members of the EU to criminalize apologetics of terrorism, which is also called the "glorification" of terrorism.[161] The European provision goes beyond true threats, recognizing that public praise, support, and justification of terrorism also pose a danger to public order.[162] *Humanitarian Law Project* does not recognize statements supporting, praising, or glorifying terror to be per se actionable offenses.[163] This distinction means that judges should not blindly follow European precedents interpreting the Convention but should use them as advisory opinions.

---

155. Crookes v. Newton, [2011] 3 S.C.R. 269, 283 (Can.); June M. Besek & Philippa S. Loengard, *Maintaining the Integrity of Digital Archives*, 31 COLUM. J.L. & ARTS 267, 311–12 (2008).

156. *See* Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers, [2004] 2 S.C.R. 427, 464–65 (Can.).

157. EUROPOL, INTERNET ORGANISED CRIME THREAT ASSESSMENT 49–50 (2016).

158. Council of Europe Convention on the Prevention of Terrorism art. 5, May 16, 2005, C.E.T.S. 196.

159. *Id.*

160. *Id.*

161. Eric De Brabandère, *The Regulation of Incitement to Terrorism in International Law*, *in* BALANCING LIBERTY AND SECURITY: THE HUMAN RIGHTS PENDULUM 233–34 (Ludovic Hennebel & Helene Tigroudja eds., 2011).

162. *Id.* at 232–34. For an example of a European case that would violate First Amendment jurisprudence, convicting someone for glorifying terror, see Sam Jones, *Jail for a Joke: Student's Case Puts Free Speech Under Spotlight in Spain*, GUARDIAN (Apr. 18, 2017), https://www.theguardian.com/world/2017/apr/18/student-cassandra-vera-tweet-case-puts-free-speech-under-spotlight-in-spain [https://perma.cc/2WX2-E8PE].

163. Holder v. Humanitarian Law Project, 561 U.S. 1, 39 (2010) (finding that the material-support "statute does not penalize mere association with a foreign terrorist organization").

CONCLUSION

Various terrorist organizations rely on social media platforms to threaten, incite, propagandize, and recruit. Internet information companies are often reluctant or ambivalent about removing even explicit and graphic calls for ideologically motivated carnage, disruption, destruction, and terrorist indoctrination. Those companies are not purveyors of threats or incitement. Their responsibility arises, nevertheless, when they cooperate with terrorist organizations by purposefully, knowingly, or recklessly providing a platform for their indoctrinating, threatening, or instructive content. In doing so, internet services can run afoul of the material-support statute. Self-policing has proven too ineffective a means for preventing the harms social media companies have created by offering terrorists digital platforms. Concerted government action by means of criminal prosecutions and injunctions is needed to maintain a national standard against the material support of designated terrorist organizations.