2017

Terrorist Incitement on the Internet

Alexander Tsesis
Loyola University School of Law

Recommended Citation
Available at: http://ir.lawnet.fordham.edu/flr/vol86/iss2/1
The internet is an astoundingly robust and dynamic instrument for all manner of communications. It is a platform for an array of webpages, blogs, chatrooms, virtual groups, news media, political forums, advertisement options, cybersleuth sites, revenge spaces, shaming discussion groups, incitement networks, and much more. While many pages on the internet are devoted to civil discourse, others are dedicated to calumnious activities. Along with newspapers and university websites, there are others engaged in cybershaming\textsuperscript{1} and cyberbullying.\textsuperscript{2}

Of even greater social, political, and cultural consequence is the slew of websites committed to the spread of hate against various groups,\textsuperscript{3} and in its darkest crevasses are terrorist websites dedicated to inciting violence, recruiting like-minded individuals, and indoctrinating others on the use of political, religious, and otherwise ideological violence.\textsuperscript{4} Terrorist speech on the internet poses a threat worldwide. The realm of communications has vastly expanded the delivery of constructive and destructive information. Groups who seek to alter governments’ policies and religious practices through havoc, violence, and intimidation are among those who exploit the cross-border nature of internet protocols and electromagnetic packets. In

\textsuperscript{*} Raymond & Mary Simon Chair in Constitutional Law and Professor of Law, Loyola University School of Law, Chicago. This Foreword provides an overview the Fordham Law Review symposium entitled \textit{Terrorist Incitement on the Internet} held at Fordham University School of Law.

1. See Patricia Sanchez Abril, \textit{A (My)space of One’s Own: On Privacy and Online Social Networks}, 6 NW. J. TECH. & INTELL. PROP. 73, 78–81 (2007) (discussing the limited capacity of tort law to provide remedies for internet posts aimed to shame a party but not rising to the falsity that must be proven for a viable slander or libel action).


addition to open propaganda on forums such as YouTube and Facebook, terrorists have increasingly exploited “darknets” to obfuscate and anonymize their activities through networks like Tor, I2P, and Freenet. While all of these are benign tools useful for confidential interactions, privacy, and other legitimate purposes, international criminals—terrorists, counterfeiters, drug dealers, and arms dealers among them—exploit these tools for nefarious purposes.

I organized this symposium to advance understanding of how terrorist communications drive and influence social, political, religious, civil, literary, and artistic conduct. Viewing terrorist speech through wide prisms of law, culture, and contemporary media can provide lawmakers, adjudicators, and administrators a better understanding of how to contain and prevent the exploitation of modern communication technologies to influence, recruit, and exploit others to perpetrate ideologically driven acts of violence. Undertaking such a multipronged study requires not only looking at the personal and sociological appeals that extreme ideology exerts but also considering how to create political, administrative, educational, and economic conditions to effect positive change at micro and macro levels. The deep analysis that a symposium provides can paint a more comprehensive picture to explain the effectiveness or ineffectiveness of various memes, videos, interactive websites, group chat rooms, and blogs that justify, glorify, or incite violence. Moreover, understanding the operation of terrorist groups on the internet can help to explain their organizational hierarchies.

Terrorist organizations’ increasingly diverse use of digital devices vastly expands their reach beyond the scope of traditional modes of communication—conversations, pamphlets, or couriers. The challenge facing government agencies and thinktanks is how to formulate policies, statutes, standards, and regulations for digital platforms that are likely to safeguard the public, while maintaining the constitutional standards of protected speech and privacy.

First Amendment values are essential for a functional democracy, personal development, and the spread of sciences. However, they do not require an absolute prohibition against national security-based restrictions. The compelling need for regulations is particularly evident when dealing with incitements to violence that are aimed at achieving political and religious ends. Terrorism is not a spontaneous reaction to the existing order; to the

7. See Neb. Press Ass’n v. Stuart, 427 U.S. 539, 570 (1976) (asserting that the “Court has frequently denied that First Amendment rights are absolute”).
8. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 160, 164–65 (1963) (asserting that the government has power to act in the interest of national security because the Constitution “is not a suicide pact”).
contrary, it requires planning, training, organizing, coordinating, executing, and debriefing for which the internet has proved to be a reliable tool.9

Among the most urgent issues confronting governments and citizens is the extent to which the state can justify censoring speech that explicitly or implicitly threatens others. One of the most respected principles of U.S. constitutional law is that the First Amendment does not prevent the government from enforcing criminal laws against speech aimed at inciting or likely to lead to an imminent harm.10 A more complex issue is the extent to which federal and state entities can censor online indoctrination that influences and directs persons to engage in future terrorist operations.

The internet differs in part from traditional communications because of the great distances that often exist between online speakers and their audiences. Rarely will a statement posted on the internet present an imminent threat of harm. However, traditional spatial and temporal considerations of imminence are insufficient for policy-makers to address internet-based terrorist incitement. Online speech likely will not present any clear or present danger—except in the rare circumstance in which the target of inciteful comments is immediately proximate to the speaker, as if, for instance, an inflammatory message was sent to someone in the immediate vicinity of the sender.11 Many terrorist threats, calls for recruitment, and virtual meetings are made from remote locations, often from countries other than the location of the audience.12 Even threats to life and physical well-being might be made to instigate others to take action at some ambiguously designated opportune time.13

The architecture of the internet creates new opportunities for the dissemination of information and the formation of groups. Joint efforts between groups with no former association often arise through digital contacts. For example, before his shooting spree and murder of American soldiers at Fort Hood in Texas, Major Nidal Hassan interacted and received encouragement from a radical Islamic imam in Yemen.14 Separately, a wife-


10. See *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam) (“[T]he constitutional guarantees of free speech and free press 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 to inciting or producing imminent lawless action and is likely to incite or produce such action.”).

11. Feiner v. New York, 340 U.S. 315, 320 (1951) (“When clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace, or order, appears, the power of the State to prevent or punish is obvious.” (quoting *Cantwell v. Connecticut*, 310 U.S. 296, 308 (1940))).


and-husband terrorist team—Tashfeen Malik and Syed Farook—pored over hours of terrorist videos on YouTube and read the Al Qaeda magazine *Inspire*. Likewise, the computer of one of the brothers who participated in the 2013 Boston Marathon bombing contained several terrorist pamphlets from abroad. These terrorists were able to connect with handlers and could obtain literature to an extent that would have been unfathomable to previous generations. All this has become possible just twenty years after the internet first became a popular tool of communication. Since the mid-1990s, communication tools have steadily developed and have been adopted by people with the best, or the worst, intentions.

Internet tools have made it easier to influence and radicalize persons who, in the past, would have found it difficult to connect with terror networks. They are part of the most disturbing aspect of internet communications and provide forums to ideologically driven violent groups in Afghanistan, Chechnya, Indonesia, Iraq, Lebanon, Malaysia, the Palestinian territories, the Philippines, Turkey, and beyond to share information about building bombs, developing terrorist cells, and perpetrating attacks. Prior to its creation, recruiters had to rely on face-to-face contacts at religious services, outdoor gatherings, and private meetings. Now, the internet has made it easier to connect and communicate with terror organizations, locate potential recruits, create and sustain ideological communities, and instigate violence.

The internet’s ability to provide quicker access to more information and to expand outreach to audiences has been invaluable to terrorists. While mainstream media such as radio, newspapers, and television stations are closed to terrorist organizations in western countries, terrorist organizations can rely on websites to dehumanize enemies and present themselves as innocent victims of powerful, colonial states.

---


21. WEIMANN, supra note 19, at 6.
The focus and function of this symposium was to assess the limits of legitimate regulations of terrorist communications spread on websites sponsored by terrorist groups, email servers, internet service providers, listservs, social platforms, and other means of cybercommunication. These subjects create one of the most pressing constitutional dilemmas of our day because of the potential consequences of misregulation. The dilemmas facing regulators are diverse and range from how to curb overbroad government regulations likely to violate the freedom of association to how to empower law enforcement to react commensurately with the evils of terrorist indoctrination and incitement.

Participants of the symposium sought to identify the categorical rules and balances that must be established by legislators and reviewed by courts to create sustainable and legally viable balances between robust protections of speech and effective safeguards for national security. In a series of panels, the authors brought their expertise to bear on the topic for elucidating. They explored whether and how government agencies should maintain content-neutral regulations across the internet while shutting down truly threatening or inciteful posts calling for the ideologically driven murder of civilians. The Articles in this issue are the result of that symposium, which I organized with the help of editors of the Fordham Law Review.

In the first article, Professor Alan Chen argues that courts should continue to apply the imminent threat of harm test established in Brandenburg v. Ohio to review regulations restricting terrorist speech. He cautions against skewing First Amendment doctrine in reaction to two distinct forms of exceptionalism. First, he expresses concern that, as has occurred in the past, the government may undermine speech protections in response to exaggerated national-security concerns. Second, he suggests that courts may similarly overreact to the possibility that changes in digital communication technologies may exacerbate those security concerns in ways that call for more robust state intervention. The nation should be particularly skeptical when the government proclaims the need to censor expression in the face of the convergence of national security and internet exceptionalism. Narrowing free speech doctrine in response to these contemporary developments, Professor Chen argues, may not only skew free speech doctrine but may also influence law enforcement agencies’ decisions to adopt invasive surveillance technologies. Professor Chen argues that in

\[22. \text{The scholars that participated in the symposium were: Jack M. Balkin, Alan K. Chen, Danielle Keats Citron, Raphael Cohen-Almagor, Caroline Mala Corbin, Matthew Fisher, Abner Greene, David S. Han, Heidi Kitrosser, Andrew Koppel, Joseph Lampau, Larissa Lidsky, Helen Norton, Martin H. Redish, Joel Reidenberg, Thane Rosenbaum, and Alexander Tsesis.}
\]

\[23. 395 U.S. 444 (1969) \text{(per curiam).}
\]

\[24. \text{Alan K. Chen, Free Speech and the Confluence of National Security and Internet Exceptionalism, 86 FORDHAM L. REV. 379, 397–99 (2017).}
\]

\[25. \text{Id. at 380.}
\]

\[26. \text{Id. at 381–85.}
\]

\[27. \text{Id. at 385–97.}
\]

\[28. \text{Id. at 397.}
\]

\[29. \text{Id.}
\]
its current form, *Brandenburg* seems appropriately calibrated to provide broad protection for pure advocacy while permitting the government to regulate speech that presents a truly imminent danger.30

Professor Danielle Citron and Brookings Institution Fellow Benjamin Wittes argue that courts have interpreted § 230 of the Communications Decency Act too broadly.31 As a result, courts have granted immunity to a variety of internet platforms even when those platforms intend to disseminate abuse and provide electronic forums for illegal conduct.32 This status quo empowers abusers to use forums with equanimity to defame, degrade, and otherwise harm victims, while the latter are left without recourse.33 Citron and Wittes propose either modification to the current judicial understanding of § 230 or legislative revision.34 Such revision would have to maintain robust speech freedoms on social media but also subject those platforms to liability when their existence is predicated on illegality ranging from defamatory claims about the sexuality of specific individuals to inflammatory terrorist assertions aimed at recruits; solicitation from site visitors for similar postings; and deliberate dissemination of such noxious content.35 Their suggested interpretation would maintain immunity for Good Samaritans while denying it to active “Bad Samaritans.”36

Professor Raphael Cohen-Almagor points out that free speech without limitations might amount to lawlessness.37 Freedom of expression is one of the most basic and important values of liberal democracies, but it needs to be weighed against an equal value—social responsibility.38 A golden mean must be identified that will provide support for both freedom of expression and social responsibility.39 Internet companies not only provide access to the internet, they also facilitate and enable speech on the internet.40 Therefore, these intermediaries have moral and social responsibilities of effective gatekeeping that help prevent violent words from becoming violent actions.41 Internet companies, as gatekeepers, should be proactive in fighting against violent speech.42 Cohen-Almagor argues that companies should act independently and proactively in preventing terrorist speech just as they do against corporate ultra vires acts.43

---

30. *Id.*
32. *Id.*
33. *Id.* at 409–10.
34. *Id.* at 415.
35. *Id.* at 417–18.
36. *Id.* at 418.
37. *Id.* at 423–24.
39. *Id.* at 434–35, 452
40. *Id.* at 434–35.
41. *Id.* at 425.
42. *Id.* at 426.
43. *Id.*
44. *Id.* at 436–38.
However, internet companies regularly fail to monitor their communication networks. Reasons they assert for this failure include a robust protection of free speech, the need for fast-paced innovation, the ambiguity of the meaning of hate speech, a commitment to avoid censorship, and the sheer volume of digital information streamed on social networks. A considerable part of this reasoning is fueled by partisan economic interests aimed to increase profits and minimize expenses. Cohen-Almagor concludes that internet intermediaries must understand that with great power comes great responsibility. Online terrorism is a grave concern; thus, due care is imperative.

Context is important in determining whether certain speech incites violence. Therefore, internet intermediaries can, and should, develop adequate algorithms to determine the context of any given message and deduce whether the speech at hand is dangerous and terrorist. In achieving this goal, cooperation with governments and security agencies is preferred to coercion. It is better for internet intermediaries to be proactive than to be coerced into action by legislatures. Cohen-Almagor believes that responsibility accompanied by enhanced technology is within reach to enable the protection of society from the ills of terrorism.

Professor Caroline Mala Corbin elaborates on, considers, and examines the effects of internet posts that depict terrorists in the United States as Muslim while simultaneously refusing to depict white people as terrorists. These false stereotypes are partly attributable to the influence of news media, which often carry sensational reports of Muslim terrorism despite the fact that more terrorist attacks in the United States are perpetrated by white extremists. Such white extremists, however, are rarely called terrorists despite being ideologically driven by a message of intimidation.

Corbin adopts critical race theory methodology to inform her awareness of subtle racism. Often, unconscious cognitive processes create racial and ethnic categories, such as the stereotype of the Muslim terrorist. Meanwhile, she asserts, caucasians enjoy white privilege, which manifests in the public perception of white terrorists as lone wolves, rather than examples

45. Id. at 430–32, 434–35.
46. Id. at 435–36.
47. Id. at 452.
48. Id. at 426–27.
49. Id. at 444–45.
50. Id. at 433 & n.63.
51. See id. at 452.
52. See id. at 452–53.
53. Id.
55. Id. at 461–62.
56. Id.
57. Id. at 462–63.
58. Id. at 464.
of endemic ethnic hatred. Corbin then examines the intersection of critical race studies and propaganda. In particular, she looks at how President Donald Trump’s administration invokes these overgeneralized narratives to disseminate propaganda that relies on cognitive social narratives that do not carefully evaluate terrorism. This propaganda contains aspects of flawed racial beliefs and advances an anti-Muslim narrative while avoiding mention of white terrorism.

Professor David Han focuses on the subset of speech of terrorist advocacy—that is, abstract advocacy of unlawful terrorist activity. That form of communication does not fall under the traditional category of low-value speech as defined by earlier U.S. Supreme Court cases. But exceptional circumstances may arise justifying regulation of such speech, and Professor Han examines how the First Amendment should account for such circumstances. He argues that courts should not immediately resort to broad doctrinal revision but rather should initially account for changed circumstances by applying strict scrutiny as is required under the current doctrinal framework. Adhering to a rigorous but meaningful strict scrutiny standard would give courts some flexibility to react in response to changed circumstances while acting as a valuable intermediate step to evaluate whether broader doctrinal reformulation is necessary. Stated somewhat differently, it gives courts a chance to carefully consider whether the present circumstances are truly indicative of a fundamentally changed reality or merely an outlier.

Professor Heidi Kitrosser’s article focuses on the federal statute prohibiting individuals from providing material support to designated terrorist organizations. She discusses lower-court opinions interpreting various provisions of the federal material support of terrorism statute. As she demonstrates, many such cases have involved expressive censorship. Kitrosser recognizes that in extreme circumstances the statute serves a worthwhile goal, but there is reason to be concerned about ambiguities in the

59. Id. at 463.
60. Id. at 466.
61. Id. at 472–80.
62. Id. at 475.
63. Id.
64. Id. at 484–85.
66. Id. at 491.
67. Id. at 493–97.
68. Id. at 498.
69. Id. at 501.
70. Id. at 507.
72. Id. at 512–17.
73. Id.
law, such as how groups are designated on the State Department’s official lists of foreign terrorist organizations and specially designated global terrorists. The principal case upholding the material-support statute, *Holder v. Humanitarian Law Project*, has created judicial superdeference to regulations against speech perceived to help terrorist organizations. Professor Kitrosser argues that the lack of adequate judicial oversight has allowed the government to use coercion to suppress constitutionally protected free expression.

Professor Andrew Koppelman argues that none of the proposed restrictions of terrorist incitement, beyond what is already unprotected, are workable. The law cannot reach internet speech that originates overseas and restrictions on reading such material do not provide readers with adequate notice of what is banned. There is also value in permitting readers to expose themselves to evil and destructive views. People may make bad choices when they are treated as adults, but free people have to be permitted to contemplate such choices.

Professor Helen Norton addresses various constitutional concerns raised by the government’s role as speaker in the War on Terror. She explains that government speech is especially powerful because of its ubiquity, variety, and reach. At times, the government’s wartime speech has a positive influence by calling for unity and healing or by informing the public about important issues. At other times, however, the government uses its wartime voice to deceive the public about its decisions or to denigrate and instill hatred against perceived outsiders. She closes by discussing a range of potential legal and policy responses to the government’s wartime fearmongering and lies.

Professor Martin Redish and Matthew Fisher draw on the strategy and conduct of terrorist organizations to evaluate whether their speech can be restricted. Such organizations engage in cybercommunications to terrorize and energize lone wolves to act on violent ideologies. Modern free speech doctrine has two strands relevant to the question of whether these terrorist

---

74. *Id.* at 520.
75. 561 U.S. 1 (2010).
77. *Id.* at 528.
79. *Id.* at 538.
80. *Id.* at 540.
81. *Id.* at 541–42.
83. *Id.*
84. *Id.* at 546.
85. *Id.* at 547–57.
86. *Id.* at 558–62.
88. *Id.* at 567–68.
communications in cyberspace can be regulated. They are the “true threats” and “incitement” doctrines.89 On the one hand, true threats are inherently coercive acts and therefore beyond the scope of the First Amendment.90 Unlawful advocacy, on the other hand, is protected under the Brandenburg incitement doctrine.91 Both doctrines are pertinent to terrorizing advocacy, which seeks to cause immediate terror in listeners analogous to a true threat.92 Yet terrorists do not simply speak in symbolic terms but aim to illicit action and trauma.93 Terror speech seeks to terrorize listeners and to induce criminal conduct.94 To deal with these threats, a model is needed to deal with hybrid speech.95 That model has three qualifications: First, the speaker must call for criminal, physical violence.96 Second, the intended victim must be aware of the threat.97 Lastly, the threat must be real, not abstract.98 If these are met, government would be allowed to suppress the nonspeech, coercive terror.99

Professor Thane Rosenbaum argues that terrorism transmitted on the internet should give us pause to reflect on how we conceptualize free speech.100 The United States is an outlier in this area of law.101 Many Americans assume that expressive interactions will always lead to meaning and truth despite evidence of real harms that speech can pose.102 Rosenbaum believes that our narcissism when it comes to extolling this fundamental liberty hampers our ability to make moral choices.103 Many people refuse to take moral positions because of free speech zealotry.104 These First Amendment absolutists, as he sees it, suffer from a form of intellectual myopia: they put ideology ahead of considerations of public safety and even common sense.105 Fascism can clearly emerge from internet anonymity and animus.106 This is not a marketplace of ideas.107 Tranquility and security stand on an equal plane with speech.108 Indeed, a people imprisoned by terror have lost all claim and capacity to exercise their freedoms.109 In this manner,
harms caused by terrorist speech delivered on the internet should be regarded with the same exclusion from First Amendment protection as any other clear, present, and imminent danger.110

Professor Alexander Tsesis’s article concentrates on terrorists’ widespread adoption of social media platforms.111 As terrorist networks increasingly embrace new media, internet information companies often remain reluctant or ambivalent about removing even explicit and graphic calls for ideologically motivated carnage, disruption, destruction, and terrorist indoctrination.112 While those companies are not purveyors of threats or incitement,113 their responsibility nevertheless arises when they cooperate with terrorist organizations by providing a platform for their indoctrination, threats, and instructive contents.114 With an increasingly proliferating number of terrorist webpages, self-policing has proven ineffective.115 However, in certain circumstances, internet services can run afoul of the material-support statute.116 Using this statute, concerted government-led criminal prosecutions and injunctions are needed to maintain national and international standards against the material support of designated terrorist organizations.117 However, just as increased government enforcement is critical for stamping out terrorist incitement, so too must the government guarantee rigorous free speech protections through government transparency, procedural safeguards, clearly defined designations, and judicial review.118

110. Id.
112. Id. at 609.
113. Id. at 616.
114. Id. at 615–16.
115. Id. at 610.
116. Id. at 619.
117. Id. at 620–28.
118. Id. at 628–30.