BRANDENBURG v. TWITTER

Michael J. Sherman*

INTRODUCTION

Decided in 1969, Brandenburg v. Ohio1 set a standard for protection of speech that remains in effect today. According to the Supreme Court, speech advocating even extreme ideas may only be proscribed when it is intended to incite imminent lawless activity and is likely to do so.2 Brandenburg explicitly overturned the Court’s ruling in Whitney v. California,3 and effectively overturned McCarthy Era decisions such as Dennis v. United States,4 which had set a much lower bar for the government in prosecuting speech.5 The Brandenburg rule puts the United States at the forefront internationally when it comes to speech protection. Other countries—including our allies—are far more willing to place restrictions on speech by extremist groups or speech that is thought to incite violence.6

Brandenburg is not without its critics, questioning whether it is sensible to create such an enormous impediment to prosecuting potentially dangerous expression.7 One example of such allegedly hazardous speech is related to the emergence of social media as an

* LL.M. Georgetown University Law Center; J.D. The University of Michigan. The author is an attorney with the federal government. The views expressed here are solely his own.

2 See id. at 447.
3 274 U.S. 357 (1927).
5 Brandenburg, 395 U.S. at 447-49.
6 See infra notes 135-73 and accompanying text.
7 See, e.g., Alexander Tsesis, Prohibiting Incitement on the Internet, 7 VA. J. L. & TECH. 5, 20 (2002) (“In taking the position that anti-incitement laws are constitutional only when they limit immediately dangerous expressions, the Court ignored a plethora of empirical evidence about the long-term effects of racist and ethnocentric propaganda.”); S. Elizabeth Wilborn Maloy & Ronald J. Krotoszynski, Jr., Recalibrating the Cost of Harm Advocacy: Getting Beyond Brandenburg, 41 WM. & MARY L. REV. 1159, 1217 (2000) (“Federal courts’ current application of the Brandenburg test to speech that advocates harm does not strike the proper balance when the speech at issue advocates lawless behavior in a manner that does not necessarily cause any imminent danger, but nevertheless poses a grave risk of directly facilitating grossly antisocial behavior.”).
important force: Twitter and Facebook are used by terrorist groups to both recruit new members and to call for violence. To the extent that these efforts are successful, they present a challenge to the federal government’s counterterrorism strategy. This article will consider some alternatives to the Brandenburg standard, including civil lawsuits—as opposed to criminal prosecution—as a means of pressuring social media companies to restrict the use of their services by terrorists. While I believe that the nature of the Internet and online speech calls for some reconsideration of Brandenburg’s imminence requirement, efforts to significantly overhaul the Brandenburg paradigm raise more problems than they solve.

I. BACKGROUND: THE BRANDENBURG RULING AND ITS APPLICATION IN THE AGE OF SOCIAL MEDIA

Clarence Brandenburg was a leader of a Ku Klux Klan group in Ohio. He was convicted of violating Ohio’s Criminal Syndicalism Act in the aftermath of a speech he gave at a Klan rally. In this speech, he said, among other things, that the Klan was “not a revengent organization, but if our President, our Congress, our Supreme Court, continues to suppress the white, Caucasian race, it’s possible that there might have to be some revengeance taken.” Despite Brandenburg’s claim that “[t]he Klan has more members in the State of Ohio than does any other organization,” the Klan rally at which Brandenburg spoke was small—the Court’s opinion describes a scene of “12 hooded figures.” The event came to the attention of law enforcement only because Brandenburg notified a local television reporter, who accepted the Klansman’s invitation to attend and record the rally, footage which was later broadcast on the reporter’s station to a local audience.

By the time Ohio authorities made the decision to prosecute Brandenburg, they were aware that the rally had taken place and nothing had happened afterward—though obviously the Klan has a

---

9 See id. at 444-45.
10 Id. at 446.
11 Id.
12 Id. at 445.
13 See id.
long history of violence.\textsuperscript{14} Even more so, by the time the case reached the Supreme Court several years later,\textsuperscript{15} it was that much clearer that the rally had attracted little notice and had scant impact.\textsuperscript{16} As noted above, Brandenburg was prosecuted under Ohio’s Criminal Syndicalism Act,\textsuperscript{17} which prohibited advocacy of “the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform.”\textsuperscript{18} The law did not have a likelihood of harm requirement.\textsuperscript{19} Instead, advocacy of “criminal syndicalism” was sufficient to convict.\textsuperscript{20} As the Court’s opinion pointed out, the Ohio law was passed as a part of a wave of such laws adopted in the period immediately following World War I.\textsuperscript{21} The intended targets of such laws were leftist radicals—people more like Anita Whitney, who was convicted under California’s Criminal Syndicalism Act,\textsuperscript{22} than Clarence Brandenburg.\textsuperscript{23}

Although Brandenburg was hardly a sympathetic figure, his sentence—a fine plus a jail sentence of one to ten years—may have seemed excessive, given what actually happened, or, rather, did not happen.\textsuperscript{24} On these facts, perhaps the Court felt more comfortable allowing wide latitude for hateful speech. It is also possible that the Court viewed the case through the lens of perceived overreaction to the threat of Communism and the excesses of the McCarthy Era. The reality of the “threat” was emphasized by Justice Douglas in his con-

\begin{itemize}
  \item \textsuperscript{14} See Brief for Appellant at 7, Brandenburg v. Ohio, 395 U.S. 444 (1969) (No. 492).
  \item \textsuperscript{15} The rally at which Brandenburg spoke took place on June 28, 1964. See Brief for Appellant at 6, Brandenburg v. Ohio, 395 U.S. 444 (1969) (No. 492). The Supreme Court noted probable jurisdiction on November 18, 1968, more than four years later. See Brandenburg v. Ohio, 393 U.S. 948 (1968).
  \item \textsuperscript{16} Although to Brandenburg’s critics cited above, even if there is no immediate reaction to speech of the sort made at a Klan rally, this does not mean that there is definitively no “harm” that can be associated with the speech. See supra note 7. Even if those critics are correct, it is still the case that Brandenburg’s speech appears not to have reached an especially wide audience.
  \item \textsuperscript{17} OHIO REV. CODE ANN. § 2923.13.
  \item \textsuperscript{18} See Brandenburg v. Ohio, 395 U.S. 444, 444-45 (1969).
  \item \textsuperscript{19} See id.
  \item \textsuperscript{20} Id.
  \item \textsuperscript{21} See id. at 447.
  \item \textsuperscript{22} See Whitney v. California, 274 U.S. 357, 359 (1927).
  \item \textsuperscript{24} See Brandenburg v. Ohio, 395 U.S. 444, 445 (1969).
\end{itemize}
curring opinion, in which he wrote that in earlier cases decided by the Court, “the threats were often loud, but always puny.”

The first important follow-up cases to Brandenburg also involved situations where there was no violence that could be directly, immediately tied to the defendant’s speech. In Hess v. Indiana, the defendant had been convicted for shouting to protesters at an anti-war rally that they would “take the fucking street later.” Though in upholding his conviction the Indiana Supreme Court claimed to be following Brandenburg, there was no evidence that Hess’s statement had affected the crowd. It appears that he was arrested largely because a police officer heard him say “fuck.” As the Supreme Court’s opinion noted, two trial witnesses indicated that they did not believe that Hess was actually urging the crowd to go back into the street. Thus, the Court concluded that what he said “at worst . . . amounted to nothing more than advocacy of illegal action at some indefinite future time. This is not sufficient to permit the State to punish Hess’s speech.”

The Court might have had a harder time reversing the Indiana Supreme Court’s decision had the demonstration turned violent. As with Brandenburg, the Court issued its ruling in Hess via a per curiam opinion, though this time three justices dissented, Justice Rehnquist’s opinion taking issue with the majority’s characterization of the relevant facts.

Similarly, in NAACP v. Claiborne Hardware, the Court overturned a damage award against the NAACP for allegedly threatening potential customers of the respondent and other local merchants.

---

25 Id. at 454 (Douglas, J., concurring). In his Dennis dissent, Justice Douglas had made a similar point, dismissively referring to the defendants as the “miserable merchants of unwanted ideas.” Dennis v. United States, 341 U.S. 494, 589 (1951) (Douglas, J., dissenting).
27 Id. at 107.
29 See id. at 419 (Hunter, J., dissenting).
30 See id. at 418.
33 See id. at 105; Brandenburg v. Ohio, 395 U.S. 444, 444 (1969). Brandenburg’s being a per curiam opinion appears to be an accident of history. The case was originally assigned to Justice Fortas, who unexpectedly resigned shortly before the decision was due to be issued. Justice Brennan made some modifications to Fortas’s draft, and then the Opinion was released unsigned. See Bernard Schwartz, Justice Brennan and the Brandenburg Decision – A Lawgiver in Action, 79 JUDICATURE 24, 28 (1995).
2018]  

BRANDENBURG v. TWITTER  

131

The key had been an NAACP official apparently\(^{36}\) saying during the course of a demonstration that if anyone patronized certain merchants, “we,” presumably representatives of the NAACP or their allies, would “break your damn neck.”\(^{37}\) Although some violence had occurred related to the boycott of local businesses,\(^ {38}\) there was no evidence that tied it directly to the speech at issue.\(^ {39}\) The Court overturned a Mississippi state court’s award of damages to the plaintiffs for lost business,\(^ {40}\) with Justice Stevens writing for the Court that “[a]n advocate must be free to stimulate his audience with spontaneous and emotional appeals for unity and action in a common cause. When such appeals do not incite lawless action, they must be regarded as protected speech.”\(^ {41}\) Unlike in \textit{Hess}, there was not a dissent, though Justice Rehnquist only concurred in the result and Justice Marshall did not participate.\(^ {42}\)

Aside from the lack of actual violence tied to the speech of the defendants in each of these cases, the speeches share something else in common: they were given to relatively small, contained crowds. In Hess’s case, it did not appear that very many people heard him at all.\(^ {43}\) Only Brandenburg’s speech was recorded, but even then it is not evident that it reached an especially wide audience.\(^ {44}\) Thus, there are at least two significant characteristics that make online recruitment of terrorists different: the ability to reach mass audiences is vastly greater than it was a generation or two ago, and there may be greater violence tied to the speech in question.

As to contact with potential recruits, two points are important. First, a tweet or online publication—such as \textit{Inspire}\(^ {45}\) magazine—can

\(^{36}\) As the Court notes, there was no recording of this speech. \textit{See id.} at 902.

\(^{37}\) \textit{Id.}

\(^{38}\) \textit{See id.} at 904-05.

\(^{39}\) \textit{See id.} at 928.

\(^{40}\) \textit{See id.} at 931-32.


\(^{42}\) \textit{See id.} at 934; \textit{see also Hess v. Indiana}, 414 U.S. 105, 109 (1973) (Rehnquist, J., dissenting).

\(^{43}\) While the state produced two witnesses who had heard Hess, they also stated that he had not spoken in a louder tone of voice than others present at the demonstration. \textit{See Hess}, 414 U.S. at 107.

\(^{44}\) Especially because, as the opinion notes, the audio for much of the recording was unclear. \textit{See Brandenburg v. Ohio}, 395 U.S. 444, 446 (1969).

reach millions of people with the click of a button. Second, a recruiter situated anywhere in the world can contact a potential recruit located thousands of miles away. As is now known, Anwar al-Aulaki had online contact with both “Underwear Bomber” Umar Farouk Abdulmutallab and Fort Hood killer Nidal Hassan.\footnote{See Dina Temple-Raston, \textit{Officials: Cleric Had Role in Christmas Bombing Attempt}, NPR (Feb. 19, 2010), http://www.npr.org/templates/story/story.php?storyId=123894237.} The \textit{Brandenburg} Court could not have imagined the progress that would be made in communication over the next forty years—even the \textit{Claiborne Hardware} Court, in 1982, would not have anticipated the coming information revolution. Wholly apart from the fear of another 9/11, the seeming ease with which smaller scale attacks have been conducted—including Hassan’s and the San Bernardino attack in 2015\footnote{On December 2, 2015, two individuals opened fire during a San Bernardino County Department of Public Health event, killing 14 people. The perpetrators were said to be inspired by exposure online to foreign terrorist groups. \textit{See} Richard A. Serrano, Paloma Esquivel, & Corina Knoll, \textit{Marquez and Farook Plotted Campus and Freeway Attacks, Prosecutors allege}, \textit{L.A. Times}, Dec. 17, 2015, http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-marquez-20151217-story.html.}—have likely increased the fear that Americans have about the ability of speech advocating criminal conduct to succeed. Although Abdulmutallab was ultimately unsuccessful, he came perilously close to ending the lives of almost 300 people.\footnote{On December 25, 2009, Abdulmutallab unsuccessfully attempted to bring down a Northwest Airlines flight by sneaking explosives onto the plane in his underwear. \textit{See} Charlie Savage, \textit{Underwear Bomber Sues Over Treatment in Supermax Prison}, \textit{N.Y. Times}, Oct. 19, 2017, https://www.nytimes.com/2017/10/19/us/politics/underwear-bomber-lawsuit-prison-treatment.html.}

One might ask whether \textit{Brandenburg} and its progeny came to us from a time and place that has changed too dramatically for the law not to change with it. Professor Lyrissa Lidsky writes, “\textit{Brandenburg}’s sanguine attitude toward the prospect of violence rests on an assumption about the audiences of radical speech. \textit{Brandenburg} assumes that most citizens (even Ku Klux Klan members) simply are not susceptible to impassioned calls to violent action by radical speakers.”\footnote{Lyrissa B. Lidsky, \textit{Incendiary Speech and Social Media}, 44 \textit{Tex. Tech. L. Rev.} 147, 160 (2011).} If that assumption breaks down, perhaps \textit{Brandenburg} does as well.

The dynamics of social media contact may also change things. Does the ability of the speaker to protect his anonymity contribute to
more violent rhetoric? And how is the audience’s reaction affected by their being alone when receiving the message? Although a throng hearing a speech may resort to mob violence, it is also possible that the crowd may exert a moderating influence on an individual who might otherwise react violently.

Professor Lidsky suggests that an individual sitting at home, alone, receiving a message, may be more likely to engage in violence as a result, even without a crowd to egg him on. She writes that the anonymity of such communications “fosters a sense of disinhibition in those contemplating violence.”

In an article in Notre Dame Law Review, Professor Thomas Healy argues that we can already see lower courts backing away from Brandenburg—even before the existence of social media—while still claiming to adhere to it. He points to cases in the Second Circuit, and the California Court of Appeals, where the courts in question upheld convictions that a commonsense reading of Brandenburg would not seem to allow. In United States v. Rahman, defendant Sheik Omar Abdel Rahman was convicted of a variety of terrorism related charges, including solicitation of murder and bombing. Some of the charges were tied to the 1993 bombing of the World Trade Center. In its opinion, the Second Circuit upheld Rahman’s conviction without “consider[ing] whether [the defendant’s] statements were directed to inciting imminent unlawful conduct or were likely to lead
to such conduct." Instead, the court held that “[w]ords of this nature—ones that instruct, solicit, or persuade others to commit crimes of violence—violate the law and may be properly prosecuted.”

In the California case, People v. Rubin, an appellate court sustained a conviction for inciting violence against an upcoming demonstration that was scheduled to take place five weeks after the speech in question. The court explained that

in these days of the global village and the big trumpet the line between advocacy and solicitation has become blurred; and when advocacy of crime is combined with the staging of a media event, the prototype images tend to merge . . . . When, as here, political assassination is urged upon a greatly enlarged audience, the incitement to crime may possess a far greater capacity for civil disruption than the oral harangue of a mob in the town square . . . .

Furthermore, the court explained that the charges had to be evaluated in light of the risk of the harm advocated: “[t]he threat to civil order presented by advocacy of assassination must be realistically evaluated in the light of its potential for deadly mischief.” This sounds far closer to Judge Learned Hand’s standard in United States v. Dennis, discussed below, than it does to Brandenburg.

These cases aside, Healy’s main exhibit for the claim that lower courts are not being faithful to Brandenburg is the case of Ali al-Timimi. Al-Timimi was an American computer programmer. In the aftermath of the 9/11 attacks, and as the US was preparing to invade Afghanistan, he informed a group of young Muslim men of a recently issued fatwa obligating all Muslims to defend Afghanistan against the coming invasion. As a means of fulfilling this obligation,
he encouraged them to fly to Pakistan to receive military training, and at a later meeting offered advice on how to reach their destination. Although the men did go to Pakistan, they eventually returned to the US without participating in hostilities.

On these facts, al-Timimi was sentenced to life imprisonment plus seventy years, the judge rejecting, among other things, a First Amendment defense based on *Brandenburg*. As Healy notes, “it is not clear that al-Timimi’s words were directed to producing lawless conduct,” because travel to Pakistan was legal and the group that provided the training had not yet been declared a terrorist group. Plus, there was little support for a claim that al-Timimi’s comments to the group were intended to incite imminent lawless action or that they did so. “And yet a federal judge rejected [al-Timimi’s] free speech claim without even writing an opinion.” Thus, although these decisions represent a small sample size, Healy is perhaps right that lower courts may prove to be looser with *Brandenburg*, especially in cases seemingly linked to terrorism. And, apart from these two cases, in the Supreme Court’s two follow-up cases to *Brandenburg* discussed above, the Court held that the lower courts in question had not correctly applied *Brandenburg*, either.

Thus, one option for the government in addressing online terrorist recruitment is simply to hope that courts will continue to be less than faithful to *Brandenburg*. Or, the government could try to bring a case to the Supreme Court that allows it to explicitly revise *Brandenburg*. Such an attempt could well be successful. It is notoriously difficult to predict how a future Supreme Court will address a particular problem, but the Justices might decide that the new realities of

---

70 Id.
71 Id. at 677.
72 Id. at 678.
73 Healy, *supra* note 54, at 678.
74 Id. at 679.
75 Id. at 680.
76 In August 2015, the Fourth Circuit remanded al-Timimi’s case to the District Court, though over evidence withholding, not on First Amendment grounds. See United States v. Al-Timimi, No. 14-4451 (4th Cir. Aug. 4, 2015) (order granting defendant’s motion to remand). As of this writing, the case remains open in the Eastern District of Virginia.
77 In this context, it is a little ironic to discuss the al-Timimi case as part of this line of cases, because this was not an example of online incitement. Al-Timimi did things the old-fashioned way, speaking directly to a small group. See Healy, *supra* note 54, at 658.
social media require a re-thinking of incitement and imminence standards established in 1969.

II. MODIFYING BRANDENBURG

There are other approaches to the issue of how to treat Brandenburg, or perhaps how to circumvent or revise it. A few recent law review articles have suggested that online recruiters could be prosecuted under the Material Support statute, 18 U.S.C. § 2339. The statute has two main sections, 2339A and 2339B. The former bans “provid[ing] material support or resources or conceal[ing] or disguis[ing] the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section [a laundry list of criminal statutes],” although the latter prohibits providing or attempting to provide “material support” to “foreign terrorist organization[s]” (FTOs). What is the “material support” that an online recruiter is trying to provide an FTO? Personnel. And attempting to provide an FTO with personnel is specifically prohibited by the statute.

Both by the terms of the statute and the Supreme Court’s ruling upholding it, the government would still be forced to show some

---

81 See Stacey, supra note 78, at 221 (“If an American has taken a ‘substantial step’ to solicit an innocent person to provide personnel . . . to ISIS, then that American should be subject to criminal prosecution under the Material Support statute.”).
83 Subsection (h) specifically exempts those who act independently of a terrorist group, even when such individuals advance the group’s goals. See id.
84 Holder v. Humanitarian Law Project, 561 U.S. 1, 8 (2010). The plaintiffs in this case challenged the constitutionality of the Material Support statute, calling it violated their First and Fifth Amendment rights. See id. The Court upheld the statute, even though it was undisputed that the plaintiffs wished to provide support to the legal activities of two designated terrorist groups, see id. at 14-15, rather than, for example, providing them with weapons. The Court found this distinction irrelevant, noting that, in writing the statute, Congress had not required “specific intent to further [an] organization’s terrorist activities.” Id. at 16-17.
level of coordination between social media accounts and an FTO. However, it is unclear how tough a standard this is for the government to meet. Consider United States v. Mehanna. Here, the First Circuit ruled that sufficient evidence of “coordination” existed where Mehanna had merely attempted, unsuccessfully, to travel to an al-Qaeda training camp. Beyond prosecuting Twitter users, others have speculated about the possibility of holding social media companies accountable under the statute. Interestingly, at least one commentator has argued that online recruitment is no more, and perhaps even less, dangerous than other forms of soliciting personnel. Among other reasons for this is that the distance and lack of connection involved in online exchanges may make it harder for the recruiter to gain the trust of his target.

Professor Lidsky, though admitting that replacing Brandenburg is challenging, has suggested modifying the imminence requirement so as to account for the realities of social media communications. This would involve attempting to show a “direct” link between the online

---

85 See id. at 3-4 (“[S]ervice . . . refers to concerted activity, not independent advocacy.”) (internal citation omitted).
86 735 F.3d 32 (1st Cir. 2013).
87 See id. at 50. As Professor Marty Lederman has noted, ruling that Mehanna’s attempt to find the training camp was enough to convict enabled the court to avoid the question of whether his work translating publicly available jihadist materials and encouraging others to engage in jihad was sufficiently “coordinated” with al-Qaeda to uphold his conviction on that basis alone. See Marty Lederman, Avoidance of the First Amendment Questions in the Mehanna Case, JUST SECURITY (Nov. 14, 2013, 8:44 AM), https://www.justsecurity.org/3174/avoidance-amendment-questions-mehanna-case/.
88 See, e.g., Susan Klein & Crystal Flinn, Social Media Compliance Programs and the War Against Terrorism, 8 HARV. NAT’L SEC. J. 53, 86-87 (2017) (advocating for a new provision in the Material Support statute that would include penalties for social media companies that did not create effective monitoring of their use by terrorists); Emily G. Knox, The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists, 66 HASTINGS L. J. 295, 308 (2014) (arguing that Section 2339B could be used to prosecute social media companies, at least in cases of individuals who identified themselves in their profiles as “acting on behalf of” a foreign terrorist organization).
89 See Steven R. Morrison, Terrorism Online: Is Speech the Same as it Ever Was?, 44 CREIGHTON L. REV. 963, 965 (2011) (“Contrary to many assumptions, cyberspace may not be a boon to terrorist organizations that seek to recruit others. Rather, [online exchanges] may have characteristics that actually hinder the recruitment process.”).
90 See id. at 999.
91 See Lidsky, supra note 49, at 161-62; see also Russell L. Weaver, Brandenburg and Incitement in a Digital Era, 80 MISS. L. J. 1263, 1287 (2011) (“Since Brandenburg was developed during a period when most subversive advocacy was delivered through speeches or printed circulars, the imminency requirement may have made more sense as applied to those methods of communication.”).
speech in question and specific acts of violence, and whether the violence in question was foreseeable, taking into account such things as the target audience and any detailed instructions by the speaker pertaining to specifically contemplated acts, as opposed to broader, vaguer calls for violence.\footnote{See Lidsky, supra note 49, at 161-62.}

This might make a difference in a narrow category of cases where the victim was identifiable from the speech in question. Professor Lidsky makes her proposal in the context of United States v. Turner,\footnote{See United States v. Turner, 720 F.3d 411 (2d Cir. 2013); cert. denied, 135 S. Ct. 49, reh'g denied, 135 S. Ct. 698 (2014).} in which Hal Turner was convicted for making threats against judges of the Seventh Circuit, a specific, identifiable victim group.\footnote{See id. at 415-16; Lidsky, supra note 49, at 157-58.} Although the district court relied on Brandenburg to affirm the jury’s decision to convict Turner,\footnote{See United States v. Turner, No. 09-00650, 2009 WL 7265601, at *2-3 (E.D.N.Y. Oct. 5, 2009).} when the case was appealed to the Second Circuit, that court turned to the “true threats” doctrine to uphold the conviction.\footnote{Turner, 720 F.3d at 419-25.} This rule allows a state to proscribe “those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.”\footnote{Virginia v. Black, 543 U.S. 343, 359 (2003); see also Turner, 720 F.3d at 420. Though the district court had ruled that Turner’s speech was unprotected under Brandenburg. See Turner, 2009 WL 7265601, at *3.} Consistent with the district court’s opinion, Lidsky argues that Turner’s statements could have been considered criminal under Brandenburg’s incitement standard.\footnote{See Lidsky, supra note 49, at 158-59.} The Second Circuit held that, because Turner’s speech constituted a true threat, it did not have to consider whether it met Brandenburg’s incitement and imminence benchmark.\footnote{See Turner, 720 F.3d at 425 (“Turner’s conduct was reasonably found by the jury to constitute a threat, unprotected by the First Amendment; it need not also constitute incitement to imminent lawless action to be properly proscribed.”).} But even if Professor Lidsky is correct, it is questionable whether such analysis could be extended to many of the general calls for violence against, for example, any available American targets.\footnote{Her position received a hint of support from Judge Rosemary Pooler, who dissented in Turner. Judge Pooler took the position that the speech did not constitute a true threat, but might have been unprotected under Brandenburg. Though she ultimately declined to reach the Brandenburg question, she quoted from a section of the district court’s opinion which found...} Instead, it would likely be limited to a...
relatively small number of situations in which a target could be pinpointed with some degree of specificity from the speech in question. Given that such cases would likely be covered by the true threats doctrine, it is hard to see how much more this gets us.

Focusing less exclusively on the imminence requirement and instead turning to the level of harm that certain speech has the potential to cause, Professors Eugene Volokh and Healy have each suggested that free speech rules be modified in cases where the speech in question could be tied to “extraordinary” levels of harm.\textsuperscript{101} Professor Volokh fears that the balance of security and freedom established by the Bill of Rights and judicial decisions interpreting it only operates sensibly in the realm of “ordinary dangers,” and may not be workable for perils that are “orders of magnitude greater.”\textsuperscript{102} As a result, he concludes that “avoiding extraordinary harms—especially harms caused by information that helps others construct nuclear and biological weapons, weapons that can kill tens of thousands at once—may justify restrictions on speech that would facilitate the harms.”\textsuperscript{103} What would such a limitation look like? “The government might, for instance, prohibit publication of certain highly dangerous information, even when the information is generated by private entities that have never signed nondisclosure agreements with the government.”\textsuperscript{104}

It is clear that Professor Volokh is at least a bit uneasy with the costs of such a rule. He admits that it could easily interfere with scientific research, public policy debates, and even our ability to have needed discussions on how to stop those seeking to inflict “extraordinary” harms.\textsuperscript{105} Perhaps even more importantly, what he proposes would “require more unchallenged trust of the government than free speech law normally contemplates.”\textsuperscript{106} Nonetheless, he concludes that

\begin{quote}
"unpersuasive" Turner’s claim that his speech was not meant to incite imminent lawlessness because he did not make it while standing outside the Seventh Circuit Courthouse. United States v. Turner, 720 F.3d 411, 434-36 (2d Cir. 2013); cert. denied, 135 S. Ct. 49, reh’g denied, 135 S. Ct. 698 (2014) (Pooler, J., dissenting).
\end{quote}

\textsuperscript{101} Eugene Volokh, Crime-Facilitating Speech, 57 STAN. L. REV. 1095, 1209-10 (2005); see also Thomas A. Healy, Brandenburg in a Time of Terror, 84 NOTRE DAME L. REV. 655, 719-21 (2009).

\textsuperscript{102} Id. at 1210.

\textsuperscript{103} Id. at 1210.

\textsuperscript{104} Id.

\textsuperscript{105} See id. at 1210-11.

\textsuperscript{106} Id. at 1211. Volokh wrote these words in 2005; perhaps he would be less willing to place greater “unchallenged trust” in government in 2017.
so long as this exception only applies in very limited situations, in cases “widely understood as being far outside the run of normal circumstances,” it is acceptable as a means of protection.107

Professor Healy, though claiming that Brandenburg “provides the proper level of protection” to extremist speech,108 cites approvingly Volokh’s article and takes a similar line: “when the harm is cata

strophic—mass casualties, enormous destruction of property, major disruption to the economy—we can, without substantially eroding free speech and without venturing too far on the slippery slope, give the government more leeway to prevent the harm from occurring.”109 From this starting point, he reaches the conclusion that “the government can prohibit advocacy of extraordinary harm if there is a ‘reasonable chance’ that the harm will result.”110 He describes this “reasonable chance” benchmark as being less stringent than a “sub

stantial chance” standard, but more so than a showing of a mere “theoretical possibility” of great harm.111 Although the focus here is primarily on the level of harm involved, Healy also asserts that in such extraordinary harm situations in wartime, Brandenburg’s likelihood and imminence requirements should not apply.112

What is interesting about Professor Healy’s proposed solution is that it brings to mind Judge Hand’s formulation in his opinion for the Second Circuit in United States v. Dennis, the forerunner to the previously mentioned Dennis Supreme Court decision a year later.113 Judge Hand explained that courts “must ask whether the gravity of the ‘evil,’ discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger.”114 In its own Dennis ruling, the Supreme Court plurality noted with approval Judge Hand’s approach.115 Given the generally negative view of Dennis 65 years after the fact,116 it would seem odd to propose a return to it,117 and

107 See id.
108 Healy, supra note 54, at 731.
109 Id. at 721.
110 Id.
111 Id.
112 See id. at 727.
113 183 F.2d 201, 212 (2d Cir. 1950), aff’d, 341 U.S. 494 (1951).
114 Id.
116 See, e.g., Jamal Greene, The Anticanon, 125 Harv. L. Rev. 379, 396 (2011) (discussing Dennis as a candidate to be included in the “anticanon,” cases so egregiously wrong that they continue to be important teaching cases simply for their wrongness); Richard A. Primus, Canon,
indeed, Professor Healy writes that “[w]ith Brandenburg and Dennis thus hopelessly at odds, which should prevail? The answer is Brandenburg.” But he does appear to recommend something similar to what Judge Hand envisioned: the government can act if the harm is serious enough and above some threshold of likeliness to occur.

Another possible, though ultimately problematic, approach comes from the Supreme Court’s jurisprudence on speech integral to criminal conduct. This doctrine stems from a 1949 decision, Giboney v. Empire Storage & Ice Co., in which the Court upheld an injunction barring the defendant from picketing plaintiff’s plant in an attempt to prevent plaintiff from selling ice to non-union ice peddlers. The Court rejected a First Amendment challenge to the Missouri law, explaining that the First Amendment does not “extend[ ] its immunity to speech or writing used as an integral part of conduct in violation of a valid criminal statute.”

This doctrine has been used in recent years to justify, among other things, restrictions on child pornography, as well as gay conversion “therapy.” So why not argue that speech encouraging terrorism is “integral” to its taking place? Volokh asserts that this approach is made more difficult by the Supreme Court’s ruling in Holder v. Humanitarian Law Project, which upheld a restriction on speech, but only after applying strict scrutiny. In Giboney, the content of the speech was not critical to the outcome because the Missouri law banning the type of picketing at issue was legal, and the defendants were not immunized from obeying the law on the basis that their law breaking included expressive elements. In Humanitarian Law Project, the content of the speech was very much at issue—it

Anti-canon, and Judicial Dissent, 48 DUKE L. J. 243, 250-51 n.33 (1998) (discussing Dennis as an example of a case whose dissenting opinions have eventually won the day).

Though Healy acknowledges that, as Dennis has never been formally overruled, its doctrine could be revived. See Healy, supra note 54, at 727-28.

R
is not per se illegal to speak with a terrorist organization, only to provide it with certain types of assistance, so the substance of what is said matters.\footnote{See Humanitarian Law Project, 561 U.S. at 27 (noting that liability under the Material Support statute depended on whether plaintiffs were attempting to impart the groups with a “specific skill” or “specialized knowledge,” as opposed to mere “general or unspecialized knowledge”). The plaintiffs claimed they wanted to advise the two designated terrorist groups on how to engage in various forms of legal political advocacy. See id. at 14-15.} In such situations, the Court ruled that it will apply strict scrutiny.\footnote{See id. at 28; see Volokh, supra note 123, at 1017.}

Although strict scrutiny is a hard standard to meet, the Court went on to hold that the government had done so, ruling that the restriction was sufficiently narrow\footnote{See Humanitarian Law Project, 561 U.S. at 39.} and justified by the government’s compelling interest in preventing terrorism.\footnote{See id. at 28; Volokh, supra note 123, at 1017 n.197.} The Court only mentioned Giboney briefly, in part because the government’s attempt to rely on it was halfhearted.\footnote{See Volokh, supra note 123, at 1017-18. Volokh discusses Humanitarian Law Project, 561 U.S. at 27 n.5, which noted that the government argued “in passing” that under cases like Giboney, any speech coordinated with a terrorist group was not protected by the First Amendment, as “speech effecting a crime.” Because the Court upheld the Material Support statute, it did not need to address this argument. As Volokh writes, given that the Court only upheld this particular use of the Material Support statute after applying strict scrutiny, it seems unlikely that the Court would have accepted the government’s view that the speech in question was wholly outside the protection of the First Amendment.} So, it is not especially clear how fruitful an avenue this would provide for additional prosecutions, especially because causation seems much more difficult to establish. In Humanitarian Law Project, the issue was a legal question, whether offering the groups in question assistance in engaging in legal activities should be prosecutable.\footnote{See Humanitarian Law Project, 561 U.S. at 15.} It was undisputed that the plaintiffs wished to provide the assistance—they brought the suit themselves as a pre-enforcement action.\footnote{See id.} Had the plaintiffs been prosecuted, the government would not have had to show that their contribution was “integral” to illegal activity.

Having to show that something on social media is “integral” to criminal activity seems like a tall order. Save the case of a Tweet or Facebook posting along the lines of “the bomb is in location x. Here is what you need to do to detonate it in location y at time z,” how would a prosecutor show that a particular Tweet or Facebook entry was “integral” to a given act of violence? What level of specificity
would be sufficient? Would repeated messages directed to a given person be enough? What if a large number of messages came from a group of people? Would they all be criminally liable? What if speech is unintentionally integral to criminal activity?

III. A BRIEF LOOK AT SOME EUROPEAN AND GLOBAL APPROACHES

As noted above, the United States is an outlier when it comes to the extent of its protection for freedom of speech, especially speech that advocates lawlessness or might incite violence. These differences also show up when it comes to speech by terrorist groups or their supporters. Among anti-terrorism laws passed in the United Kingdom are the Terrorism Act 2000\textsuperscript{135} and the Terrorism Act 2006,\textsuperscript{136} the latter of which was passed in the aftermath of the London subway bombing of 2005. The provisions of the 2000 law include sections which ban membership in or supporting a list of organizations alleged to be tied to terrorism.\textsuperscript{137} While initially the banned groups were largely connected to the conflict over Northern Ireland, more recent additions include groups tied to international terrorism.\textsuperscript{138} Professor Adam Tomkins points out that this provision of UK law goes further than America’s material support law upheld in \textit{Humanitarian Law Project}, in that it bans mere membership in the listed organizations.\textsuperscript{139} In 2016, 260 people were arrested under the 2000 law and related statutes, down from 282 the year before.\textsuperscript{140}

The 2006 Act prohibits statements that “[are] likely to be understood . . . as a direct or indirect encouragement . . . of acts of terrorism . . . .”\textsuperscript{141} The Act further allows punishment for statements that

\textsuperscript{135} Terrorism Act 2000 (Eng.).

\textsuperscript{136} Terrorism Act 2006 (Eng.).

\textsuperscript{137} See Terrorism Act 2000, c. 11, §§ 11(1), 12(1)(a).


\textsuperscript{139} See \textit{id.} at 87 n.33 (citing Holder v. Humanitarian Law Project, 561 U.S. 1, 18 (2010)).


“glorify” acts of terrorism,142 including sentences of up to seven years.143 Additionally, the law has a section banning transmission of documents that glorify or encourage terrorism.144 Tomkins comments that “[t]his is an offense that is designed to have an impact on free speech.”145 Even apart from the UK not having the countervailing balance of a basic law like the First Amendment, its statute instantly gives much broader latitude to British law enforcement. The speech in question must only be “indirect” advocacy of terrorism, and need not even be intended as such by the speaker. There is no imminence requirement; the state does not have to prove that the statement was likely to result in illegal activity.

The UK’s law is so far-reaching that it was criticized by the United Nations Human Rights Committee, which oversees implementation of the International Convention on Civil and Political Rights (ICCPR).146 The Committee expressed its concern that the crime of encouraging terrorism was defined in “broad and vague” terms, and could even be used to convict in circumstances where the speaker did not intend his speech to be taken as encouragement to terrorism.147 The Committee recommended that the law be amended so as to avoid “a disproportionate interference with freedom of expression.”148

French law bans speech which “provoke[s] discrimination, hatred, or violence” against an individual or group on the basis of several categories, including race, religion, and ethnicity.149 This law appears to have been enforced more aggressively in the aftermath of the Charlie Hebdo attacks.150 French comedian Dieudonné M’Bala M’Bala was arrested, convicted, and fined merely for expressing sympathy with the Hebdo attackers as well as those who attacked a Jewish supermar-

142 Renieris, supra note 141, at 687; Terrorism Act 2006, c. 11, § 1(2)(a) (Eng.).

143 Terrorism Act 2006, c.11, § 1(7)(a).

144 See id. at § 2; see also Ellen Parker, Implementation of the UK Terrorism Act of 2006 – the Relationship Between Counterterrorism Law, Free Speech, and the Muslim Community in the United Kingdom Versus the United States, 21 EMORY INT’L L. REV. 711, 716-17 (2007).

145 Tomkins, supra note 138, at 89.


147 HRC Report, supra note 146, at 71.

148 Id.


150 See Uddin, supra note 149, at 197 (“On one hand, the government upheld Charlie Hebdo as a bastion of free speech, and on the other hand, it brutally cracked down on contrarians.”).
ket around the same time. There was no evidence that his comments were intended to, or had, incited additional attacks, or were meant to do anything beyond outrage sensibilities and draw attention to the speaker. Indeed, even intending to outrage need not be proven under French law, much less actual incitement; “prosecutors and courts [can] punish individuals on the basis of mere speculation that the speech could incite a terrorist act.” As with Britain, the Human Rights Committee also expressed concern with French anti-terrorism law, in particular its increased use after the Hebdo attacks in prosecutions of minors for “vindication” of terrorism.

Spain also criminalizes “glorifying” terrorism. Article 578 of its Penal Code, like Britain’s, bans glorification of terrorism, and also penalizes demeaning the victims of terrorism and their families. Professor Shawn Boyne writes that the Spanish law is “even more susceptible to overbreadth problems than the United Kingdom’s provisions.” Defendants under the Spanish law have included: a rock band for lyrics that allegedly glorified terrorists, a woman who tweeted about a Spanish Prime Minister killed in 1973, and two puppeteers. The New York Times reports that prosecutions under this Article have increased markedly in recent years. Spanish police actively search social media sites, looking for speech that can be sanctioned under Article 578. In at least some cases, arrests have been made on the basis of expressions of support for separatist indepen-

---

151 See id. at 189-90.
154 See Código Penal [C.P.] [Penal Code] art. 578 (Spain). For translation, see Boyne, supra note 152, at 457.
155 Boyne, supra note 152, at 460.
156 See id. at 461 (internal citation omitted).
159 See id.
idence movements within Spain. Similar to England and France, Spain’s legislation in this area attracted the notice of the Human Rights Committee. The Committee stated its fears over the “deterrent” effect on freedom of expression of the Spanish law, especially because of “vague and ambiguous terms in some provisions, which could give rise to wide variations in the implementation of the Act.” Amnesty International also weighed in in a recent report, noting that “[t]he offence of ‘glorifying terrorism’ continued to be used to prosecute people peacefully exercising their right to freedom of expression.”

Article 10 of the European Convention on Human Rights protects freedom of expression, including the right to “receive and impart information and ideas without interference by public authority.” However, this language is significantly limited by the second paragraph of Article 10, which allows for restrictions “in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

Furthermore, Boyne asserts that the European Court of Human Rights, making use of the “margin of appreciation” concept, whereby member states are given some degree of latitude to adapt continent-wide statutes to their own particular circumstances, will allow nations more and more flexibility in applying the Convention, thereby leading to increased curbs on expression. In perhaps a sign of what is to come, the Euro-

---

161 See Belen Fernandez, Spain Versus Twitter, Al-Jazeera, May 7, 2014, http://www.aljazeera.com/indepth/opinion/2014/05/spain-versus-twitter-2014569152147223.html. This, of course, is different than the American standard the Supreme Court set out in Humanitarian Law Project, where it held that speech (or other activities) had to be coordinated with a terrorist group in order to run afoul of the Material Support statute. See supra notes 84-87 and accompanying text.


164 Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, ¶ 1, Nov. 4, 1950 (Europ.).

165 Id. at ¶ 2.

166 See Boyne, supra note 152, at 446.

167 See id. at 468-69.
pean Commission recently criticized Twitter for not removing hate speech quickly enough from its platform.\footnote{See Mark Scott, Twitter Fails E.U. Standard on Removing Hate Speech Online, N.Y. TIMES, May 31, 2017, https://www.nytimes.com/2017/05/31/technology/twitter-facebook-google-europe-hate-speech.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=EndOfArticle&pgtype=article.}

Beyond Europe and the United States, international law addresses incitement in the ICCPR, to which the US is a party.\footnote{International Covenant on Civil and Political Rights art. 19(2), Dec. 19, 1966, S. Exec. Doc. No. 95-2, 999 U.N.T.S. 171 [hereinafter ICCPR].} The ICCPR has a free speech provision, Article 19, which, in language akin to the European Convention, declares that the right to free expression “shall include freedom to seek, receive and impart information and ideas of all kinds.”\footnote{ICCPR art. 19(2), Dec. 16, 1966, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171.} But also similar to the European Convention, expressive rights under the ICCPR are subject to important limits. The treaty takes the position that the right to free speech “carries with it special duties and responsibilities,”\footnote{Id. art. 19(3).} and may be restricted for a number of reasons, including to protect national security.\footnote{See id. art. 19(3)(b).} Furthermore, Article 20(2) states that “[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.”\footnote{Id. art. 20(2).} Thus, were the US to follow the ICCPR’s approach, it might be able to prosecute terrorist recruiters on those grounds as well, though it should be noted that when the US ratified the ICCPR, it did so with a reservation that it would not apply any treaty provisions that conflicted with the First Amendment.\footnote{See S. Rep. No. 102-23, at 6-7 (1992) https://www.state.gov/documents/organization/235639.pdf. The UK, France, and Spain did not issue similar reservations concerning the limitations on speech in the ICCPR. See ICCPR, supra note 169, at c. IV, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en#EndDec.} There is certainly no shortage of alternatives, were the United States to abandon the \textit{Brandenburg} standard. But would any of these be an improvement? And perhaps more importantly, would any of them be better for the American government as an anti-terrorism strategy, or would they eventually come to be viewed as an overreac-
tion by government, typical throughout American history during times of crisis.\footnote{See, e.g., \textit{David Cole and James X. Dempsey, Terrorism and the Constitution} 1 (2006) ("The record of our nation’s response to the threat of political violence is unfortunately one of repeated infringements of [political freedom, due process, and protection of privacy]."); \textit{Geoffrey R. Stone, Perilous Times: Free Speech in Wartime, From the Sedition Act of 1798 to the War on Terrorism} 5 (2004) ("[T]he United States has a long and unfortunate history of overreacting to the perceived dangers of wartime.").}

\section{Jurisdictional and Technological Issues}

To be sure, there are problems beyond the question of what legal standard to follow. The first, and perhaps most obvious, is that many of the online recruiters are overseas, beyond American jurisdiction. Although, as some have noted, this points to the need for some sort of internationally coordinated response.\footnote{See, e.g., Weaver, \textit{supra} note 91, at 1288; Tsesis, \textit{supra} note 7, ¶ 92 (calling for an international treaty prohibiting transmission of “hate speech” over the Internet).} However, it is likely to be extremely difficult to agree on a standard even among allies—the restrictions discussed above imposed by the UK, France, and Spain would certainly not be acceptable under American law, for example—much less among hostile countries.\footnote{See \textit{Weaver, supra} note 91, at 1288.} One can only imagine negotiations between the United States and nations such as China, Syria, Russia, Iran, and Turkey over how to police online recruitment.

Aside from jurisdictional issues, there is an important technological one: encryption. Although encryption can be useful to protect, for example, secure transactions and critical infrastructure from attack,\footnote{See Hugh J. McCarthy, \textit{Decoding the Encryption Debate: Why Legislation to Restrict Strong Encryption Will Not Resolve the “Going Dark” Problem}, 20 J. INTERNET L. 1, 17-18 (2016).} increasingly extremists are turning to encryption as a means of shielding their communications from the prying eyes of government. One recent article speaks of the “widespread adoption of encryption technologies [by terrorists] to hide their communications, in an attempt to evade law enforcement and plot future attacks without any—or at most a greatly diminished—risk of detection.”\footnote{Jamil N. Jaffer & Daniel J. Rosenthal, \textit{Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge}, 24 CATH. U. J. L. & TECH 273, 274-75 (2016).} In congressional testimony, then-Federal Bureau of Investigation (FBI) Director James Comey described the ability of such individuals to make use of...
encryption as a “grave” and “growing” threat to national security.\textsuperscript{180} Former George W. Bush administration official Jamil Jaffer and former Obama administration official Daniel Rosenthal conclude that “the growing trend towards default-on, ubiquitous strong encryption, while providing critically important privacy and security benefits, also means the United States is more likely to face challenges in preventing the next major terrorist attack in the West.”\textsuperscript{181}

There have been proposals to restrict the use of encryption, or to make it breakable in certain situations.\textsuperscript{182} As Irish practitioner Hugh McCarthy explains, proponents of such limitations assert that government simply cannot fulfill its basic duty to protect its citizens without the ability to overcome encryption.\textsuperscript{183} However, he argues that legislative controls on encryption will not stop bad actors from availing themselves of the technology,\textsuperscript{184} but will make legitimate systems weaker, by, in effect, building a flaw into the system that can be used not only by legitimate law enforcement but by hackers as well.\textsuperscript{185} Jaffer and Rosenthal propose an encryption version of the post-9/11 “know your customer” banking regulations that the Department of Treasury has enforced to great effect in restricting terrorists’ access to the worldwide banking system.\textsuperscript{186} The idea is that, just as the Treasury regulations have allowed the US to “designate” non-compliant banks, the US would now be able to “designate” internet service providers that did not allow some sort of law enforcement access to encrypted communications. With this, the hope being that this would allow the US to “effectively drive encrypted terrorist communications off of the international communications grid, regardless of the jurisdiction in

\textsuperscript{180} Id. at 291.
\textsuperscript{181} Id. at 276-77.
\textsuperscript{182} See, e.g., McCarthy, supra note 178, at 19-20; Benjamin Wittes, An Out of the Box Approach to the Going Dark Problem, L A W F A R E, (Feb. 2, 2016, 11:49 AM), https://www.lawfareblog.com/out-box-approach-going-dark-problem (arguing that immunity for internet service providers from claims related to things written by users should be conditioned on the company’s ability to break encryption in response to a lawful court order).
\textsuperscript{183} See McCarthy, supra note 178, at 22.
\textsuperscript{184} See id. at 23.
\textsuperscript{186} See Jaffer & Rosenthal, supra note 179, at 308.
which the designated entity maintains its base of operations.” 187 Still, it is unclear at this time how viable legislation is as a long-term solution. Instead, the fear is that attempts to defeat encryption will lock government into a never-ending fight with terrorists over who has the best and newest technology, with serious costs to the economy and to personal privacy. 188

V. STOPPING THE PROBLEM BEFORE IT STARTS: “COUNTERING VIOLENT EXTREMISM” PROGRAMS

An approach employed by several government agencies goes under the label of “countering violent extremism,” or CVE. 189 The idea is that in addition to whatever efforts the government takes to prevent acts of violence or to bring charges against those planning or inciting such attacks, government should take an active role in dissuading individuals who might otherwise be recruited to carry out attacks. 190 “CVE counters the ideological recruitment, focusing on the root causes of many terrorist motivations, and working to prevent those causes, or provide ‘off-ramps’ for individuals who may have taken steps toward embracing ideologically motivated violence.” 191 Unlike criminal law enforcement efforts, CVE does not rely on coercion, but is voluntary. 192

In addition to an emphasis on understanding the root causes behind radicalization, CVE programs include working both with individuals who appear to be at risk of radicalizing, as well as those who may have already committed acts of violence, to re-integrate them back into the larger society. 193 Whether a good idea or not, the CVE approach, of course, does not depend upon the continued vitality of Brandenburg, much less agreement upon something to replace it. The US is hardly alone in looking to CVE as a means to combat extremist violence. 194 According to a 2015 estimate, there may be more than

187 Id.
188 See McCarthy, supra note 178, at 23-24.
189 George Selim, Approaches for Countering Violent Extremism at Home and Abroad, 668 ANNALS AM. ACAD. POL. & SOC. SCI. 94, 95 (2016).
190 Id.
191 Id. at 95.
192 See id.
193 See id. at 96; see also Kelly A. Berkell, Off-Ramp Opportunities in Material Support Cases, 8 HARV. NAT’L SEC. J. 1, 5-7 (2017).
194 See Berkell, supra note 193, at 27-28.
three-dozen programs around the world, in countries ranging from Saudi Arabia to Denmark. 195

The FBI has embraced CVE. It has created a public website, “Don’t Be a Puppet,” which attempts to inform potential recruits about the methods used by terrorists, and to convince those thought susceptible to such recruitment to avoid entangling themselves in dangerous activities. 196 Other agencies, including the Department of Homeland Security 197 and the State Department, 198 also have CVE programs. 199

But these efforts have not come without controversy. The FBI’s CVE work has been criticized in some parts of the public interest community. 200 There is concern about whether CVE is an appropriate mission for a criminal law enforcement agency. 201 After an episode in which the FBI was found to have sent an informant into a mosque in Los Angeles, 202 as well as the revelation that training sessions provided by the FBI contained materials found to be biased and offensive, 203 there is a lack of trust between some communities and law enforcement, which might make it difficult for the FBI to be effective with CVE.


201 See Bjelopera, supra note 199, at 12 (quoting a Muslim Public Affairs Council official as saying that “people cannot be suspects and partners at the same time”) (internal citation omitted).


203 See Bjelopera, supra note 199, at 14-15.
To some of its critics, government CVE programs have focused too heavily on radicalization within Muslim communities, and not enough on right-wing extremism.\textsuperscript{204} Even apart from this more specific complaint, others have attacked the whole notion of CVE on the grounds that attempts to predict who will and will not become radicalized and violent are likely to be both inaccurate and discriminatory,\textsuperscript{205} and that the studies that CVE programs are based on are thinly sourced, at best.\textsuperscript{206} In a 2011 report, New York University Law School’s Brennan Center for Justice asserted that “[d]espite the impetus to find a terrorist profile or hallmarks of radicalization to hone in on incipient terrorists, empirical research has emphatically and repeatedly concluded that there is no such profile and no such easily identifiable hallmarks.”\textsuperscript{207} Professor Amna Akbar writes that as CVE programs have proliferated, when it comes to actual cases, “a growing number of national security prosecutions target political and religious speech,”\textsuperscript{208} specifically referencing the aforementioned Mehanna case as an example.\textsuperscript{209}

VI. PUBLIC PRESSURE AND CIVIL LITIGATION AGAINST SOCIAL MEDIA COMPANIES

Another non-criminal law enforcement approach has been to attempt to convince social media companies to attack the problem themselves. This pressure has come in at least two different ways: public campaigns to get the companies to track and police or even shut down extremist accounts,\textsuperscript{210} and lawsuits against these companies.

\textsuperscript{204} See Berkell, supra note 193, at 17-18. Though as Berkell notes, there are others who take the opposite position, namely that CVE programs have not concentrated enough on Islamic extremism, in an effort at political correctness. See id. at 18-19.

\textsuperscript{205} See id. at 17.


\textsuperscript{207} Faiza Patel, Brennan Center for Justice, Rethinking Radicalization 8 (2011).

\textsuperscript{208} Akbar, supra note 206, at 828.

\textsuperscript{209} See id. at 829-831.

\textsuperscript{210} See, e.g., Micah Lakin Avni, Opinion, The Facebook Intifada, N.Y. TIMES, Nov. 3, 2015, http://www.nytimes.com/2015/11/03/opinion/the-facebook-intifada.html?_r=0. Full disclosure: Avni (who is one of the plaintiffs in the Force litigation discussed below and who has been especially outspoken on this topic) and I attended the same summer camp many years ago. See also Tech Firms, supra note 185 (asserting that “technology giants [should] take more responsibility for what appears on their networks”). At least one commentator has raised the question of whether it should be the responsibility of the media companies themselves, as opposed to the government, to identify accounts associated with terrorists. See Nina I. Brown, Fight Terror, Not
from the families of victims of terrorism. The first significant lawsuit on this front, *Fields v. Twitter*,211 (*Fields I*) was dismissed by the Northern District of California, for reasons discussed below. The district court then gave the plaintiffs an opportunity to amend their complaint,212 but the district court once again dismissed the claim, on somewhat similar grounds, as described below.213 The plaintiffs have appealed this second decision, *Fields II*, to the Ninth Circuit; the case is pending.214

The *Fields* plaintiffs were the survivors of two American contractors killed at a police training center in Jordan by a Jordanian police captain.215 Their claim was that Twitter had violated the Anti-Terrorism Act (ATA),216 by providing material support to ISIS, in violation of sections 2339A and 2339B of the Material Support statute.217 Section 2333(a) of the ATA provides a federal cause of action to any US national, or his survivors, injured by “an act of international terrorism.”218 In other words, the plaintiffs claimed that the Twitter accounts provided to those representing terrorist groups—in the plaintiffs' mind, a violation of the material support statute—in violation of the Material Support statute were the proximate cause of the injuries to their decedents, thereby providing a cause of action under the ATA.219 The surviving family members argued that merely providing accounts to terrorist organizations constituted material support to these organizations, thus making the companies subject to ATA liability.220 The plaintiffs further asserted that this was true irrespective of anything contained in actual tweets.221 This meant that Twitter became liable under Section 2333(a) the moment the accounts were established, because setting up the accounts enabled ISIS to spread its

---

211 200 F. Supp. 3d 964 (N.D. Cal. 2016) [hereinafter *Fields I*].

212 See *Fields v. Twitter*, 217 F. Supp. 3d 116 (N.D. Cal. 2016) [hereinafter *Fields II*].

213 See id.


215 See *Fields I*, 200 F. Supp. 3d at 966.


217 See *Fields I*, 200 F. Supp. 3d at 967.


220 See id.

221 See id. at 970.
message, which eventually led to the murder of the plaintiffs’
decedents.\footnote{222 See id.}

In the court’s view, the case had several flaws, among them that
the plaintiffs had not alleged, much less established, causation
between anything on Twitter and the actions of the killer.\footnote{223 See id. at 974 (“Nowhere in their opposition brief or [First Amended Complaint] do plaintiffs explain how Twitter’s mere provision of Twitter accounts to ISIS—conduct that allegedly created liability before ‘the publication of any content’ and would support liability ‘[e]ven if ISIS had never issued a single tweet,’ . . . —proximately caused the November 2015 shooting.”).} The court
also noted that the plaintiffs’ claim that mere provision of the
accounts was enough to establish liability did not fit with the rest of
their complaint, which made numerous allegations tied to the actual
content of ISIS tweets.\footnote{224 See id. at 973-74.} Thus, even if providing the accounts was
enough to make out a violation of the Material Support statute, this
would not be enough to sustain a damages claim under the ATA,
because it did not establish causation.\footnote{225 See Fields I, 200 F. Supp. 3d at 974.} The plaintiffs’ causation the-
tory was that the police captain who killed their decedents had been
“very moved” by an execution that ISIS had carried out and public-
ized on Twitter—a connection the court described as “tenuous at
best.”\footnote{226 Fields I, 200 F. Supp. 3d at 974.} The link was especially weak under the plaintiffs’ provision
of accounts theory, because liability was “based on specific content
disseminated through Twitter, not the mere provision of Twitter
accounts.”\footnote{227 Id.}

But, the biggest stumbling block to the plaintiffs’ claim was Sec-
tion 230 of the Communications Decency Act (CDA).\footnote{228 47 U.S.C. § 230 (2012).} Section
230(c)(1) states that “interactive computer service” providers, such as
Twitter, shall not be considered the “publisher” of material that

\footnote{222 See id.}
\footnote{223 See id. at 974 (“Nowhere in their opposition brief or [First Amended Complaint] do plaintiffs explain how Twitter’s mere provision of Twitter accounts to ISIS—conduct that allegedly created liability before ‘the publication of any content’ and would support liability ‘[e]ven if ISIS had never issued a single tweet,’ . . . —proximately caused the November 2015 shooting.”).}
\footnote{224 See id. at 973-74.}
\footnote{225 See Fields I, 200 F. Supp. 3d at 974. In a blog post at Lawfare discussing the Fields case, Ben Wittes and Zoe Bedell anticipated just this sort of conundrum, writing that “we think it reasonably clear that § 230 [of the Communications Decency Act] would not protect a service provider like Twitter from civil liability under § 2333 for violating the material support law (assuming it did violate it), at least if a plaintiff managed to avoid relying on the contents of tweets as evidence . . . . The trouble, of course, is that it’s pretty hard to imagine a plaintiff who could establish all of the elements required under § 2333 (particularly the causal relationship between the material support and the injury) without ever relying on the substance of third-party content.” 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.}
\footnote{226 Fields I, 200 F. Supp. 3d at 974.}
\footnote{227 Id.}
appears on their sites.\footnote{229} This provision will, for example, protect Twitter from liability if one of its users posts libelous material. In the context of social media use by terrorist organizations—or anyone else, for that matter—not only does it mean that Twitter and companies like it are not responsible for monitoring what the ISIS account says, if anything it actually encourages them to take a hands-off approach: the less that Twitter has to do with what people tweet, the less it seems like a “publisher” of the material in question. As the court explained in \textit{Fields I}, “courts have repeatedly described publishing activity under section 230(c)(1) as including decisions about what third-party content may be posted online.”\footnote{230} If you are not engaged in this decision making process, then you are not a publisher of the content.\footnote{231} Because Twitter was not a “publisher” of the information on the ISIS account, it could not be held liable.\footnote{232} In the court’s view, this was true whether the alleged wrongdoing was providing the accounts in the first place, or allowing already existing accounts to publish whatever the account holder wanted.\footnote{233}

Given a second chance, the \textit{Fields} plaintiffs were still unsuccessful in convincing the court that their claims were not barred by Section 230. The \textit{Fields II} decision covers much of the same ground as the first ruling; the court again rejected the plaintiffs’ attempts to cast their claim as content neutral and not implicating Section 230 immunity.\footnote{234} But the opinion also contains a section entitled “Plaintiffs’ Public Policy Theory,” in which the court responds to the plaintiffs’ claim that Congress had not intended CDA Section 230 to protect Twitter from giving a platform to terrorists.\footnote{235} The court begins by stating that if Congress had in fact intended to exclude this sort of material from Section 230 coverage, it should have said so,\footnote{236} but then
it moves onto a discussion of the practical impact of accepting plaintiffs’ argument:

Moreover, plaintiffs’ argument is incoherent. If the goal of the CDA is to “encourage the unfettered and unregulated development of free speech,” any policy that requires interactive computer service providers to remove or filter particular content undermines this purpose. Such a policy would require companies like Twitter to institute (1) expensive and likely imperfect content-specific controls or (2) broad content neutral restrictions that suppress content across the board. If content-specific controls are expensive enough to institute, and the penalties for failure to adequately control objectionable content are sufficiently severe, companies like Twitter will be encouraged to reduce their services or stop offering them altogether [sic].

Surely this gets at the main underlying concern with any attempt to hold service providers responsible for content posted by users. It is simply impossible for Twitter to continuously monitor postings, much less require it to decide what content is or is not acceptable. Section 230 was a reaction to a libel judgment in a New York case, *Stratton Oakmont v. Prodigy Services Co.*, in which the trial court held that the defendant could be considered the “publisher” of material posted by a third party on the defendant’s online bulletin board. So it is not surprising that a court would be hesitant to interpret Section 230 in such a way as to bring back the status quo ante.

In addition to the appeal of *Fields II* to the Ninth Circuit, in *Force v. Facebook* survivors of Hamas terrorism in Israel filed a claim against Facebook in New York. As national security writers and

---

237 *Id.* The *Fields I* opinion hints at this issue as well, but in a slightly different context, the court noting that plaintiffs’ theory that providing accounts would be enough to trigger liability “would significantly affect Twitter’s monitoring and publication of third-party content by effectively requiring Twitter to police and restrict its provision of Twitter accounts.” *Fields I*, 200 F. Supp. 3d at 973.

238 This issue is discussed in further detail below. See infra notes 247-59 and accompanying text.


240 See *id.* at *5.

241 However, the *Stratton* court justified its holding on the significant editorial control that the board operators exercised over postings, see *id.* at *4*, which differentiates it from Twitter.

bloggers Benjamin Wittes and Zoe Bedell note, the plaintiffs tried quite hard to establish causation between Facebook use by Hamas and the acts of terrorism suffered by the plaintiffs’ family members. The Force complaint argued that social media is far more effective than previously used forms of dissemination, quoting former Israeli Ambassador to the US Dore Gold as saying that “whereas ten years ago, [a] terrorist organization [like] Hamas would publish a booklet in print with limited impact, today, the same publication can be posted to Facebook and widely disseminated to rapid and devastating effect.” It also asserted that Facebook has the ability to more closely monitor the postings of groups like Hamas, pointing out that the company monitors for, and deletes, pornography. It then argued that Hamas-created videos posted on Facebook calling for attacks on Israelis have had their intended effect, including in the cases involving the plaintiffs’ decedents, especially because Facebook’s algorithms are specifically designed to connect like-minded people with one another. Because of this algorithm Hamas videos calling for suicide attacks will easily reach the right audience.

Thus, although the complaint did not allege that any of the killers tied to these particular plaintiffs stated, while being interrogated by police, that “I did it because of something I saw on Facebook,” the Force plaintiffs went to much greater lengths to establish causation than did the Fields plaintiffs. The complaint quoted Jerusalem Mayor Nir Barkat as follows: “[w]hen they interrogate the terrorists, what we see is young people who are incited to a level I have never seen before, and you see that they seek to harm innocents and listen to no one except Facebook and Twitter.” These attacks have been a key part of a terror campaign driven by Hamas’s use of Facebook to incite, enlist, organize, and dispatch would-be killers to “stab” and “slaughter Jews.”


245 See id. at 52.

246 See id. at 50-51.

247 See id. at 48-51.

248 Id. at 47.

249 Id. at 32.
praise those who have carried out attacks,250 and has also provided an outlet for those who are about to carry out attacks to discuss their intentions.251 Thus, the Force plaintiffs presented a far stronger case for causation than existed in Fields, in which the killer did not even have a Twitter account.252

In addition to the causality element, the plaintiffs also argued that Section 230 should not be a bar to recovery because they were suing over terrorist attacks that had taken place outside of the United States.253 Given the general presumption in American law against extraterritorial application of domestic statutes,254 the plaintiffs claimed that Section 230 could not provide protection for events occurring overseas.255

Despite this greater effort to establish causality and to get around CDA immunity, so far the Force plaintiffs have proved no more successful than the Fields plaintiffs. In May 2017, the Eastern District for New York dismissed the complaint, in a decision now known as Cohen v. Facebook.256 The court explained that the CDA “prevents courts from entertaining civil actions that seek to impose liability on defendants like Facebook for allowing third parties to post offensive or harmful content or failing to remove such content once posted.”257 Citing the Fields II opinion, the New York court similarly rejected the plaintiffs’ claim that their action was based merely on the provision of

250 See, e.g., Force Complaint, supra note 244, at 32.
251 See id. at 5.
252 Fields I, 200 F. Supp. 3d 964, 967 (N.D. Cal. 2016). It is worth noting that allowing victims of allegedly harmful speech to sue for damages has also been attempted with regard to pornography. In 1984, the city of Indianapolis passed an anti-pornography statute that created a right of action for those claiming to be victimized by an individual consumer of pornography. See American Booksellers Ass’n v. Hudnut, 771 F.2d 323, 325 (7th Cir. 1985), aff’d, 475 U.S. 1001, reh’g denied 475 U.S. 1132 (1986). Although the Seventh Circuit held that the ordinance was unconstitutional because it was viewpoint-based and defined pornography too broadly, see id. at 331-32, Judge Easterbrook’s opinion also stated that, under a more properly defined definition of prohibited speech, a right of action for those injured by such speech would not be objectionable. See id. at 333. The opinion theorized that had there been injuries causally attributable to Brandenburg’s speech, or the speech at issue in Claiborne Hardware, a damages award would have been appropriate. See id.
254 See Blackmer v. United States, 284 U.S. 421, 437 (1932) (“[T]he legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States.”).
255 See Pl.’s Opp’n at 31.
257 Id. at 157 (internal citations omitted).
accounts to Hamas, and not on the actual content of the accounts.\footnote{See id. ("[T]his attempt to draw a narrow distinction between policing accounts and policing content must ultimately be rejected. Facebook’s choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform.").} Wittes and Bedell correctly predicted the conundrum the plaintiffs found themselves in. They could not simultaneously establish causality and that their complaint was content neutral, the court ruling that the plaintiffs were “rely[ing] on content to establish causation and, by extension, Facebook’s liability.”\footnote{See id.} Making the substance of the postings an issue in the complaint would force “the court to treat the defendant as the publisher or speaker of content provided by Hamas,” an option foreclosed by Section 230.\footnote{Id. at 158 (internal quotations and citations omitted).}

On the extraterritoriality issue, the court agreed with the plaintiffs that the CDA lacks the indicia of intent to apply extraterritorially that is normally required before a court will extend a statute’s reach beyond American borders.\footnote{See id. at 159.} However, it also ruled that the “focus” of the CDA is limiting civil liability.\footnote{See Cohen v. Facebook, Inc., 252 F. Supp. 3d 140, 159-60 (E.D.N.Y. 2017).} In light of this, the court determined that the “relevant location” for CDA purposes is where the immunity is applied, the location of the litigation itself, not where the events underlying the claims arose.\footnote{Id. at 160.} This meant that the statute did not have to be applied extraterritorially to provide the social media defendants with the immunity the court had already determined they qualified for.\footnote{See id.}

Not surprisingly, \textit{Fields} and \textit{Cohen/Force} are not the only cases against social media companies. There has been at least one other case in the Northern District of California—\footnote{See Gonzalez v. Twitter, Inc., No. 3:16-cv-03282, at ¶¶ 1, 9 (N.D. Cal. filed June 14, 2016).}—the jurisdiction of the \textit{Fields} litigation—filed by the father of a woman killed in a Paris bistro, as well as a case filed in December 2016, in the Eastern District of Michigan by relatives of those killed in the Pulse nightclub in Orlando.\footnote{See Crosby v. Twitter, Inc., No. 2:16-cv-14406-DML-DRG, 2016 WL 7383679, at ¶ 1 (E.D. Mich. filed Dec. 19, 2016).}
In the Michigan case, the plaintiffs have attempted to get around Section 230 immunity by charging that “Defendants are information content providers because they create unique content by combining ISIS postings with advertisements in a way that is specifically targeted at the viewer.”267 In other words, the defendants are not merely providing a conduit for others to post their own statements, but are actively involved in the creation of at least some of the information in question,268 and with making sure it reaches the “right” audience.269

The plaintiffs have made the additional point that the social media companies profit from ISIS postings through their ability to specifically target advertising at those who view such postings,270 and that groups like ISIS have benefitted greatly from the existence of platforms like Twitter.271 As with the Cohen/Force plaintiffs, the Crosby plaintiffs have attempted to frame their claim as content neutral, asserting that “each Defendant derives revenue from ISIS postings irrespective of the content of ISIS’s postings.”272 It remains to be seen whether the Michigan court will be any more sympathetic to this claim than Judge Garaufis was in Cohen/Force. Although so far the plaintiffs in these suits have not been successful, we should expect such cases to proliferate until a more definitive ruling comes from a higher court.

267 Id. at ¶ 1.

268 See id. at ¶ 126 (“By specifically targeting advertisements based on viewers and content, Defendants are no longer simply passing through the content of third parties. Defendants are themselves creating content because Defendants exercise control over what advertisement to match with an ISIS posting.”).

269 See id. at ¶ 125 (“These ads are not placed randomly by Defendants. Instead, they are targeted to the viewer using knowledge about the viewer as well as information about the content being viewed.”).

270 See id. at ¶ 126 (“Defendants’ profits are enhanced by charging advertisers extra for targeting advertisements at viewers based upon knowledge of the viewer and the content being viewed.”). Perhaps in response to being exposed to just this sort of claim, Google—which owns YouTube—has been taking steps to eliminate advertising from videos with extremist content. See Daisuke Wakabayashi, YouTube Sets New Policies to Curb Extremist Videos, N.Y. Times, June 18, 2017, https://www.nytimes.com/2017/06/18/business/youtube-terrorism.html?_r=0. In addition, content that is extremist but does not qualify to be banned under YouTube policies will be marked as with a warning. See id. The company’s hope is to reduce the exposure of such videos without prohibiting them outright. See id.

271 See id. at ¶ 2.

CONCLUSION: HOW FEASIBLE IS IT TO CHANGE BRANDENBURG? WHAT WOULD THE COSTS BE?

As discussed previously, efforts to regulate or prosecute speech advocating terrorism face problems both jurisdictional—the speakers may be outside of the US—and technological—encryption, most notably. These are, to some degree, new problems. But as some of the cases discussed herein demonstrate, the old problems associated with efforts to restrict speech remain very much with us, most especially overreach—the idea that the government will always try to expand any powers it has to restrict speech, especially to the detriment of those critical of the regime—and the slippery slope—the idea that once you begin with efforts to restrict speech it is hard to stop, and more and more speech is censored, with serious costs to the free and open exchange of ideas.273 Although Hand’s formula, referenced above, might be appealing in an age where the potential evil in question seems so high, it is important to remember that it comes from a case involving the conviction of members of the American Communist Party, individuals who, in hindsight, hardly seem to have been so dangerous. It is important to be cognizant of the potential for zealous efforts at self-protection to carry too far. Every generation perceives its particular national security threat as existential.

In his Dennis plurality opinion, Chief Justice Vinson decried the notion that the First Amendment operated as a restriction “until the putsch is about to be executed,”274 suggesting real anxiety over the prospect of such an occurrence. The Japanese internments were the result of panic at the thought of a Japanese invasion of the West Coast.275 During World War I, President Wilson called for press censorship in the name of “public safety.”276 Even beyond the national security context, throughout American history the First Amendment has been challenged by those who believe, at least in some circum-

273 Professor Volokh describes a slippery slope situation as one “where decision A, which you might find appealing, ends up materially increasing the probability that others will bring about decision B, which you oppose.” Eugene Volokh, The Mechanisms of the Slippery Slope, 116 HARV. L. REV. 1026, 1030 (2003).
276 See id. at 47.
stances, it conflicts with other constitutional values and must give way.\textsuperscript{277}

In the end, efforts to radically change \textit{Brandenburg} in response to online terrorist recruitment suffer from too many defects. The jurisdictional and technological hurdles discussed above exist independently of any analysis of First Amendment doctrine. The slippery slope problem, of course, is a central conundrum of speech regulation.\textsuperscript{278} The civil suits against Twitter and Facebook highlight the enormous threat to these companies and to the free exchange of ideas if the suits are successful.

Surely the \textit{Fields} court is correct that it would be extremely expensive for social media companies to institute the kind of monitoring that would be required to truly police the sites for content that has the potential to incite, or merely encourage, acts of violence. Moreover, the plaintiffs’ comparison to Facebook’s censoring of pornography as a model that can be followed for regulating pro-terrorist messages is inapt. Justice Stewart’s famous line about obscenity, that he knew it when he saw it,\textsuperscript{279} has a certain logic here. With pornography it is not nearly as difficult to craft a policy of what is and is not acceptable, and to scan pictures to enforce the rule. But for Facebook or Twitter to commit to (a) creating a policy that determines what does and does not count as inciting; and then (b) reading every post to search for violations; and finally (c) deciding whether literally millions of posts are merely angry, strident criticism or are intended to incite illegal activity, is a vastly greater undertaking. We can already see some of the results of such efforts.

Facebook and Twitter each have policy statements on hateful or inciting material. Echoing some of the European statutes discussed above, Facebook states that it “remove[s] graphic images when they


\textsuperscript{278} See, e.g., Cohen v. California, 403 U.S. 15, 25 (1971). In his famous Opinion for the Court overturning the conviction of an individual for wearing a jacket bearing the words “Fuck the Draft” in a California state courthouse, Justice John Marshall Harlan spoke to the fundamental fear of the slippery slope in First Amendment law. Justice Harlan asked “[h]ow is one to distinguish this from any other offensive word? Surely the State has no right to cleanse public debate to the point where it is grammatically palatable to the most squeamish among us. Yet no readily ascertainable general principle exists for stopping short of that result were we to affirm the judgment below.” \textit{Id.} See also Volokh, \textit{supra} note 273, at 1029.

\textsuperscript{279} See Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).
are shared for sadistic pleasure or to celebrate or glorify violence.\textsuperscript{280} The company also will remove “hate speech,” which it defines as speech that “directly attacks people” on the basis of several categories, including “Race, Ethnicity, National origin, Religious affiliation, Sexual orientation, Sex, gender, or gender identity, or Serious disabilities or diseases.”\textsuperscript{281} Similarly, Twitter informs its customers that they “may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease. We also do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories.”\textsuperscript{282}

Even aside from the resources that it requires to enforce these policies, who decides? Who are the employees of these companies in whom we have enough confidence to make such momentous and far-reaching decisions? A recent article described Facebook employees as being “overwhelmed” by the amount of material they are required to review on a daily basis, with decisions having to be made in as little as ten seconds.\textsuperscript{283} Not surprisingly, given this description of the review process, Facebook has been criticized for not applying their current policies neutrally, unfairly—at least by the terms of their policy—favoring some groups over others,\textsuperscript{284} and also for having policies that tend to favor some groups over others.\textsuperscript{285} Members of the persecuted


\textsuperscript{282} Help Center, TWITTER, https://support.twitter.com/articles/20175050 (last visited Nov. 20, 2017).


Rohingya in Burma have found their attempts to bring attention to their plight through Facebook postings blocked by the company. See Albert F. Cahn, Facebook’s Silencing of Refugees Reveals Dangers of Censorship Technologies, JUST SECURITY (Sept. 29, 2017, 10:15 AM), https://www.justsecurity.org/45495/rohingya-censorship-demands-greater-transparency-facebook/.


“Censorship” by private companies is, of course, a vastly different matter than censorship by the government. Losing your Facebook or Twitter account is a far cry from being arrested. But that does not mean there is no cost to barring people from forums that are increasingly important to the exchange of ideas, especially in a world where governmental bodies are making ever greater use of social media (both government agencies and individual officials now have social media accounts almost as a matter of routine) to communicate with their constituents. Expanding the roles and control of the apparently overworked employees of these companies hardly seems like an ideal solution.

One anecdotal example of the impact of the enforcement of these policies: as I was editing this article, a friend posted on Facebook that the company had blocked one of her posts because it had been flagged as “offensive” by other users. What was the allegedly offensive post? A request for signatures on a petition to the US Department of Labor calling on the Department to raise the minimum wage for tipped employees.

Perhaps to address this problem, Facebook has recently announced that it will use artificial intelligence to find and remove extremist content; it remains to be seen how much of an improvement, if any, this will prove to be.

Regardless of the success of these efforts, if we create a situation where every single decision about whether a post is inciting violence is subject to being second-guessed by a jury, with millions of dollars hanging in the balance, the incentives for social media businesses...
point overwhelmingly in one direction. The end result would be inevitable. The companies would be forced to censor anything more controversial than birthday wishes and cat videos, simply out of the fear of liability. As the *Fields* court pointed out, this is an outcome directly contrary to the intent of the CDA. In the words of Professor Nina Brown:

> A finding in favor of the plaintiffs [in suits against social media companies] would, at minimum, force social media to actively monitor and police any account it suspected as having a link to a [terrorist group], but could also require much more. The repercussions would not stop with Twitter, Facebook, and YouTube (Google). All companies offering web-based services would certainly have reason to worry, as would websites that offer even attenuated support or services that are generally available to the public. The impact would be far-reaching and potentially crippling for many organizations. Further, many organizations likely would become increasingly involved with content regulation, consequently impacting the ability of the billions who use social media to communicate as openly and without [sic] as little oversight as they do now.

As if the fear of civil liability were not enough, as referenced above one recent article has even proposed an addition to the Material Support statute that would include criminal penalties for social media companies that fail to create and implement “compliance program[s]” that identify users “who may be conspiring to engage, attempting to engage, or engaging in any terrorism-related crime.” Under this proposal, the aforementioned Facebook workers spending mere seconds on thousands of posts every day would now have criminal liability for the company riding on their decisions. Private companies are not subject to the First Amendment, so overly censorious decisions are not illegal, even if they are ill-considered for other reasons. But the proposal would have the effect of asking personnel of

---

291 See Tech Firms, supra note 185 (“If internet firms are threatened with fines, they may simply remove all flagged content, just in case.”). As the article also points out, the financial burden of self-regulation would fall especially hard on newer and smaller firms, which would be unlikely to have the resources to hire sufficient staff to review all postings. See id.

292 See supra note 237 and accompanying text.

293 Brown, supra note 210, at 12.

294 Klein & Flinn, supra note 88, at 87.
these companies to correctly understand, interpret, and apply criminal statutes thousands of times a day.

Finally, there is disagreement about whether it is a good idea to force extremists off of social media at all.\textsuperscript{295} Some experts would prefer that accounts tied to terrorist groups remain visible to law enforcement.\textsuperscript{296} If forced off of the public sites, the fear is that these groups will move to programs protected by encryption.\textsuperscript{297}

All of that said, Professor Volokh is not one who generally or lightly favors speech restrictions, so it is instructive that even he is on the side of some bending of \textit{Brandenburg} in cases where the potential harm at issue is exceptionally high. The problem in carving out an exception like this is keeping it narrow enough so that it is only used in truly extreme circumstances. The question is, how do we determine what the benchmark is? For Volokh, it is situations involving the potential death of tens of thousands of people.\textsuperscript{298} By this standard, 9/11 would not have qualified as sufficiently extreme. One wonders whether it would really be possible to hold the line as Volokh proposes\textsuperscript{299} or whether “extreme” would end up being defined down. Where is the judge who will rule that an insufficient number of people are at serious risk so as to allow an established exception to be invoked? Who will argue that 2,000 lives, or even 200, are not enough?\textsuperscript{300}

A possible partial compromise position stems from the reality that in many cases in or close to Volokh’s extreme circumstances category, the speech in question will be found to be sufficiently “coordinated” with an FTO to premise prosecution on the Material Support statute. Smaller scale attacks may be doable by a lone wolf, but for

\textsuperscript{295} See Ariel V. Lieberman, \textit{Terrorism, the Internet, and Propaganda: A Deadly Combination}, 9 J. Nat’l Sec. L. & Pol’y 95, 116-17 (2017).
\textsuperscript{296} See id. at 117.
\textsuperscript{297} See id; see also How Israel Spots Lone-Wolf Attackers, \textit{The Economist}, June 8, 2017, http://www.economist.com/news/international/21723113-algorithms-monitor-social-media-posts-palestinians-how-israel-spots-lone-wolf-attackers (describing how the Israeli Army monitors social media accounts of some Palestinians in an effort to predict which individuals might be planning an attack, though also noting that this level of surveillance would likely not be possible in the US).
\textsuperscript{298} See Volokh, supra note 101, at 1211.
\textsuperscript{299} See id. Volokh suggests that cases meeting his standard “would be widely understood as being far outside the run of normal circumstances, so that they would always be seen as highly unusual exceptions to the normal rule of protection.”
\textsuperscript{300} Volokh himself essentially acknowledges this reality. See id. (“[W]hether I’m right or wrong, chances are that judges will indeed allow this sort of restriction.”).
the truly exceptional mass casualty events, it is more probable that some organization would be required, meaning that the prosecution could rest on the Material Support statute, rather than on the basis of a less speech-protective reading of Brandenburg. Thus, we may not need to alter Brandenburg to address at least some threats of significant mass casualty events.

An additional element of Brandenburg that must be considered in contemplating how or why we might choose to modify its holding in some way is the imminence requirement. As discussed earlier, speech must not only be likely to incite lawless action, but must do so “imminently.” The Court has never defined “imminence” precisely, instead noting in the aforementioned follow-up cases Hess and Claiborne Hardware that the requirement had not been met. As noted above, in Hess the Court characterized Hess’s speech as, at most, calling for illegal action at some indefinite future time, which was insufficient as a basis for prosecution. In Claiborne Hardware, the Court pointed out that no violence had occurred for “weeks or months” after the speech in question. Thus, those attempting to interpret this part of the doctrine have typically suggested that “imminent” means within a few hours, or at most, days, though, as referenced previously, the California court in Rubin found the imminence standard satisfied by a five-week timeframe.

Modern technology raises questions for how we have traditionally thought of the imminence test. Brandenburg comes to us from a time in which the capacity to replay a message repeatedly was far different. In that world, imminence was a simpler, easier to understand concept: was a speaker likely to incite immediate, or close to immediate, lawless action on the part of those to whom he was speaking? Movies and TV existed, but the ability of a particular person—especially one on the fringes of society—to reach a mass audience was

---

304 See, e.g., L. A. Powe, Brandenburg Then and Now, 44 Tex. Tech L. Rev. 69, 77-78 (2011) (“I have always taught imminence as being ‘pretty damn soon’ . . . . If my teaching has been correct, imminence is probably a matter of hours, or stretching, a few days.”); Healy, supra note 54, at 718 (arguing that “several days is the critical time period” with regard to the imminence standard).
306 See Weaver, supra note 91, at 1277 (“Brandenburg was formulated to apply to a speaker who was trying to whip a crowd into a frenzy.”).
quite limited. We now live in an era where it is far more the case that once something is recorded and put on the Internet, it never really goes away. Professor Russell Weaver suggests that, to some degree, this changed circumstance cuts both ways. The Internet makes it possible for anyone to get their message out. This may add to the danger, but also makes it easier for law enforcement to monitor such threats, although the availability of encryption has the potential to alter this to some degree. Still, if the Klan of the 1960s had been able to easily and repeatedly use Brandenburg’s speech to incite acts of violence, the Supreme Court might not have set such a high bar for imminence.

John Cronan argues that Brandenburg’s imminence requirement “does not work with the vast majority of Internet communications, as words in cyberspace are usually ‘heard’ well after they are ‘spoken.’” He suggests that “imminence” be evaluated from the perspective of the listener, rather than that of the speaker. In this scenario, a court’s job would be to determine “whether the viewer, upon reading the message, is likely to be incited to initiate imminent, lawless action,” which would require “careful scrutiny” of the message. Such scrutiny would include considering “what, if any, value the message adds to the current debate,” including whether the speech “foster[s]” or “chill[s]” debate. John Cronan, currently a Deputy Assistant Attorney General in the Criminal Division of the Department of Justice, also contends that courts should take into account the likely audience of online speech, though acknowledging that it may be difficult to do this precisely: “Although identifying the specific audience in cyberspace is often infeasible, it is possible to anticipate the likely audience of Internet messages. The identification of the likely

---

307 See id. at 1288.
308 John P. Cronan, The Next Challenge for the First Amendment: The Framework for an Internet Incitement Standard, 51 CATH. U. L. REV. 425, 428 (2002); see also Weaver, supra note 91, at 1278 (“[I]t may not seem obvious that the Brandenburg test can be meaningfully applied to communications posted on the Internet.”); Peter Margulies, The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment, 8 UCLA J. L. & TECH. 1, 53 (“The asynchronous nature of Internet time allows operatives to readily gain access to material on web-sites at their convenience.”).
309 See Cronan, supra note 308, at 456.
310 Id. at 456.
311 See id. at 457.
312 Id. at 458.
Finally, he asserts that courts should consider the issue that is at the center of the speech, and whether it is on a controversial topic that has been connected to violence:

A court’s inquiry also must look at the nature of the issue around which the alleged incitement revolves. Certain issues or controversies conjure stronger and more impassioned emotions than others. Just as a fiery speech at an anti-war demonstration is more likely to incite lawless action than one at a religious rally, Internet postings on different topics have varied effects. If it is a political debate, what is the tone of the debate? Is it a debate that has been characterized by violence?314

Professor Lidsky’s article, discussed above, suggests a reevaluation of imminence for cyber cases. But again, it is important to note the context of her article: threats against specific, identifiable individuals, which, as a result, means that incitement jurisprudence overlaps with the true threats doctrine. This is different, and far more limited, than speech which is a broad but vague call to violence against “all nonbelievers,” or all members of a particular racial or ethnic group. For speech such as this, we should consider that, in line with Cronan’s suggestion, words may be capable of “imminently” inciting long after they have initially been spoken, because of the ease with which speeches can be replayed, repeatedly. So perhaps this is one area where changed circumstances should prompt a reevaluation of Brandenburg’s imminence requirement. Surely Cronan is correct that the Internet changes the nature of speaker-listener interactions in ways the Brandenburg Court could not truly have anticipated or appreciated.

But in evaluating Cronan’s proposals, it quickly becomes apparent how complicated what he advocates would be for courts to impose, to say nothing of the possible chilling effect on speech. Take the easiest hypothetical case: a high-ranking official of a terrorist group records a message, encouraging his followers to carry out immediate attacks. The message is recorded with the understanding and intent that it will be played over and over again, and can be watched

313 Id. at 460.
314 Id. at 462. In making this argument, Cronan points to the specific example of violence at abortion clinics. See Cronan, supra note 308, at 462-64.
at the listener’s convenience, conceivably at precisely the time when a particular person is most susceptible to its message. It would perhaps not be a serious weakening of *Brandenburg* to hold that the speaker in this scenario is not immunized on lack of imminence grounds. But another speaker may simply have been caught up in the moment and lost his temper. In this scenario, even if at the moment when the words were spoken the speaker might have intended to incite, does the fact that the speech was recorded and can now be played repeatedly really mean that the speaker should be forever liable whenever his words reach the “wrong” audience?

Consider Justice Stevens’s language from *Claiborne Hardware* quoted above.\(^{315}\) Can a speaker truly be free to make “spontaneous and emotional appeals” under a regime that ties his liability wholly to the reaction of any future hearer of the speech in question? This raises a serious chilling concern. The situation sets up a new twist on the concept of the heckler’s veto;\(^{316}\) a speaker may in perpetuity be held liable, or be in fear of such liability, on the basis of the reaction of any given hearer of his speech. This is too high a cost for a speaker to bear. Instead, if courts move toward a listener centered analysis of incitement, any prosecution should have to show that a speaker intended for his speech to be used recurrently and to be used to incite in these repeated viewings. The first of the above hypotheticals is a relatively easy case; the second far less so.

Cronan’s other suggestions, that judges weigh in on the alleged “value” of speech and whether it fosters or chills debate, are not unique to this corner of First Amendment law.\(^{317}\) But they ask judges

---

\(^{315}\) See *supra* note 41, at 929 and accompanying text.


\(^{317}\) Perhaps the classic example of considering the value of speech is fighting words. In *Chaplinsky v. New Hampshire*, the Court ruled that fighting words were not protected by the First Amendment, Justice Murphy explaining that “[j]t has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.” 315 U.S. 568, 572 (1942). But the Court has never sustained another conviction under this doctrine. Or consider the Court’s struggles with commercial speech. In *Valentine v. Chrestensen*, the Court held that commercial speech was not protected by the First Amendment. 316 U.S. 52, 54 (1942). But in *Virginia Pharmacy Board v. Virginia Consumer Council*, not only did the Court strike down a restriction on consumer speech, Justice Blackmun’s majority opinion observed that such allegedly low-value speech might in fact be more valuable to its audience than types of speech previously thought to be central to the First Amendment: “As to the particular consumer’s interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the day’s most urgent
to make rulings that are inherently subjective and unpredictable, and which courts in the past have struggled with. Such uncertainty is inherently chilling for speakers, who will censor themselves if it is unclear where the lines are.

Caution in imposing new restrictions is particularly appropriate at this point in our history. At the height of the Cold War, Justice Robert Jackson said the following in a speech: “it is easy, by giving way to passion, intolerance and suspicions of wartime, to reduce our liberties to a shadow, often in answer to exaggerated claims of security.”

Justice Jackson, of course, dissented in *Korematsu v. United States* from the Supreme Court’s affirmance of one of the most serious (and now discredited) “reductions of liberty” in American history, the Japanese internments during World War II. As uncalled for as the internments were, they were undertaken within the scope of a declared war, that was understood to have had a beginning, and would presumably have an end as well, at which time those held would be released.

We now find ourselves in the War on Terror. Although this war has had at least two fairly well-defined and identified battlefronts, Afghanistan and Iraq, it is an ongoing fight against a shifting enemy that does not appear to have a conclusion in sight. What this means is that any reduction in protection for civil liberties cannot be so easily defended as a necessary, temporary response to a short-lived emergency. As Professor Geoffrey Stone has written:

“If Bush is right that this war will slog on in perpetuity, that is all the more reason to be scrupulous in scrutinizing proposed restrictions of civil liberties. The fear of perpetual war can be seen as a reason to strip away all “unnecessary” civil liberties, but the opposite is true. Apolitical debate . . . . Those whom the suppression of prescription drug price information hits the hardest are the poor, the sick, and particularly the aged.”

Obscenity is another example of “low-value” speech where the Court has, to put it mildly, found it difficult to develop consistent, easily applicable standards. On the chilling/facilitating question, judicial debates as to what speech chills other speech and what speech furthers additional debate seem unlikely to lead to any clearer path forward, with the possible exception of speech which threatens specific individuals, though as already noted, such speech is likely to be proscribable as a true threat, without having to alter our understanding of *Brandenburg*.

---


saving “grace” of America’s past excesses is that they were usually of short duration. Once the crisis passed, the nation returned to equilibrium. A war of indefinite duration, however, seriously increases the risk that “emergency” restrictions will become a permanent feature of American life.320

It is instructive to note that the book in which Stone penned these words came out a decade ago. We appear no nearer to the end of the War on Terror now than we did then. Thus, if we are to establish inroads into previously established protections for civil liberties, we cannot defend them as temporary measures; they must be acceptable in times of war, peace, and what we might think of as long-term “semi-war.” Furthermore, given the frequent tendency in times of military conflict to rush to impose restrictions on speech, it is especially important for courts to be aggressive in defending individual rights. Stone, again: “[a]lthough Congress and the president have often underprotected civil liberties in wartime, there is not a single instance in which the Supreme Court has overprotected those liberties in a way that caused any demonstrable harm to the national security.”321

At most, then, we are left with a modification to the imminence requirement that takes account of the realities of the Internet and social media322 at least under some circumstances. This is a suggestion that, as it were, tugs at Brandenburg at the margins. And that is appropriate. For all our concerns about terrorism, or whatever new threats may emerge in a future age, history has shown that it is exceedingly difficult to limit free speech without significant costs, including overzealous prosecutions of individuals who represent no real threat, such as Dennis and M’Bala M’Bala, and serious risks to the ability of forums for the exchange of ideas, such as Facebook and Twitter, to exist at all. We should tread carefully.

320 Stone, supra note 275, at 129-30 (emphasis in original).
321 Id. at 180 (emphasis in original).
322 Though, interestingly, Cronan’s article pre-dates the existence of sites like Twitter and Facebook.