NOTE

MONITORING "INSPIRATION": FIRST AMENDMENT LIMITATIONS ON SURVEILLING INDIVIDUALS WHO VIEW TERRORIST PROPAGANDA

Katherine Kaiser Moy*

* J.D. 2018, Stanford Law School. I am deeply grateful to the discerning and meticulous editorial staff of the *Stanford Law & Policy Review*, particularly Jimmy Ruck, Jon Collier, Kyle Grigel, Paige Whidbee, and Ashwin Aravind. Any errors remain my own doing.

INTRODUCTION

On June 29, 2016, a twenty-nine-year-old security guard named Omar Mateen walked into Pulse, a gay nightclub in Orlando, Florida, and opened fire. Over the course of several hours, he killed forty-nine people and injured dozens more.[1] During a 9-1-1 call in the midst of the attack, Mateen announced his allegiance to the so-called Islamic State—also known as the Islamic State of Iraq and Syria (ISIS)—a jihadist terrorist organization.[2] At the time, the incident was the worst mass shooting in modern U.S. history.[3]

Mateen was not unknown to law enforcement. More than three years before the attack, Mateen's co-workers at the St. Lucie County Courthouse reported to authorities that he had claimed to be connected to al-Qaida and Hezbollah, and had said that he wanted to "die as a martyr."[4] Upon receiving this tip, the local sheriff's office alerted the FBI, which opened a preliminary investigation into Mateen's activities. FBI agents deployed virtually every tool legally available to verify that he posed no threat to those around him.[5] They ran Mateen's name through a "maze of federal criminal and terrorism databases" and checked his phone records for any suspicious contacts.[6] They followed him in unmarked vehicles for an unspecified amount of time.[7] They "deployed two confidential informants more than two dozen times" to record his conversations.[8] And they even interviewed him twice.[9]

---

1. Mark Mazzetti, Eric Lichtblau & Alan Blinder, *Omar Mateen, Twice Scrutinized by F.B.I., Shows Threat of Lone Terrorists*, N.Y. TIMES (June 13, 2016), https://nyti.ms/2lnVJGM.

2. Rukmini Callimachi, *Was Orlando Shooter Really Acting for ISIS? For ISIS, It's All the Same*, N.Y. TIMES (June 12, 2016), https://nyti.ms/2mQkt9V.

3. Del Quentin Wilber, *The FBI Investigated the Orlando Mass Shooter for 10 Months—and Found Nothing. Here's Why*, L.A. TIMES (July 14, 2016), http://www.latimes.com/nation/la-na-fbi-investigation-mateen-20160712-snap-story.html. The Pulse attack remained the deadliest shooting in modern U.S. history until October 2017, when Stephen Paddock opened fire on concertgoers in Las Vegas, killing fifty-nine people. *See* Lynh Bui et al., *At Least 59 Killed in Las Vegas Shooting Rampage, More Than 500 Others Injured*, WASH. POST (Oct. 2, 2017), http://wapo.st/2ySKPz8?tid=ss_tw&utm_term=.32f3 06f f6631.

4. Wilber, *supra* note 3.

5. FBI procedures limit applications for surveillance under the Foreign Intelligence Surveillance Act (FISA) to "full investigations." *See* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 143 (2013), https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2013-version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202013%20Version%20Part%2001%20of%2001/view. It is not clear why Mateen's case was never elevated to a full investigation.

6. Wilber, *supra* note 3.

7. *Id.*; *see also* United States v. Jones, 565 U.S. 400 (2012).

8. Wilber, *supra* note 3; *see also* United States v. White, 401 U.S. 745 (1971) (holding that an informant's recording and transmission of a conversation without the suspect's knowledge did not constitute a "search" under the Fourth Amendment).

But the FBI found nothing. As one investigator explained, "[w]e went right up to the edge of what we could do legally, and there was just nothing there."[10] Mateen admitted to the FBI's informants that he had told his coworkers he was tied to terrorist organizations, but claimed he was just bluffing, trying to scare them after they teased him about his religion; his co-workers corroborated the story.[11] After ten months, the FBI concluded its investigation in mid-2014.[12]

A few months later, the FBI got another chance—they interviewed Mateen about a former member of his mosque who had carried out a suicide bombing in Syria. Based on a tip from another mosque attendee,[13] agents asked Mateen if he had watched any videos of Anwar al-Awlaki, the American al-Qaida propagandist who was killed in a U.S. drone strike in Yemen in 2011. Mateen denied watching the videos,[14] and the FBI moved on.[15]

More than two years later, in the aftermath of the attack on the Pulse nightclub, it was obvious that the FBI had missed something. Post-shooting analysis of Mateen's computer revealed that he had viewed terrorist propaganda videos online, including some depicting beheadings. He had also sought information about ISIS on the Internet.[16] Short of this fact, however, nothing the FBI could have known during its earlier investigation suggested Mateen was likely to conduct an ISIS-"inspired" attack. A review of Mateen's social media accounts revealed no direct connections to terrorist groups.[17] He had never posted statements indicating sympathy with terrorist causes before the night of the attack. And there was no evidence he had ever coordinated with the group in preparation for the attack.

Attacks carried out in the name of—but not planned by—terrorist organizations are a reality in the age of ISIS. This past October, twenty-nine-year-old Sayfullo Saipov drove a truck into a crowd in Manhattan, killing eight people.[18] Investigators discovered photos of ISIS's leader on Saipov's phone,

---

9. Wilber, *supra* note 3; *see also* Oregon v. Mathiason, 429 U.S. 492 (1977) (holding that a voluntary interrogation at a station house was not a "custodial interrogation" that entitled the suspect to the protections of Miranda v. Arizona, 384 U.S. 436 (1966)).

10. Wilber, *supra* note 3.

11. *Id.*

12. *Id.*; Mateen's name was removed from a terrorist watchlist at the conclusion of the FBI's initial investigation. Mazettti et al., *supra* note 1.

13. Wilber, *supra* note 3.

14. *Id.*

15. The FBI had no "further contact" with Mateen, and there is no indication that he was subject to further monitoring. Mazettti et al., *supra* note 1.

16. *Id.*

17. *Id.*

18. Devlin Barrett, Matt Zapotosky & Mark Berman, *New York Truck Attack Suspect Charged with Terrorism Offense*, WASH. POST (Nov. 2, 2017), http://wapo.st/2gTWOos?tid=ss_tw&utm_term=.259c04d8bdb7. Saipov's use of a truck as a weapon echoed the style of attack other ISIS supporters had used in Europe on several occasions since 2016. *See, e.g.*, Greg Myre, *As ISIS Promotes Vehicle Attacks, Terrorists Strike in Europe and U.S.*, NPR (Nov. 1, 2017, 12:35 PM ET) (mentioning an attack in Nice, France in July 2016 and Barcelona, Spain in August 2017).

as well as a note near the scene bearing a slogan believed to refer to the group.[19] ISIS claimed responsibility for the attack a few days later.[20] In December 2015, a married couple killed fourteen people at an office holiday party in San Bernardino, California, shortly after one of the attackers pledged allegiance to ISIS in a Facebook post.[21] Indeed, the concept of the "ISIS-inspired" attack increasingly dominates the public conception of terrorist threats.[22] As the events of September 11, 2001 become a more distant memory, and the United States and its allies continue to dismantle al-Qaida operational networks and safe-havens, these comparatively unsophisticated yet persistent attacks can chip away at our sense of security.

The Pulse attack helped reveal that law enforcement and intelligence professionals may not be properly equipped to prevent these attacks with the tools available to them under the law. Perhaps if the FBI had been able to monitor Omar Mateen's online activity to confirm that he had watched propaganda videos of beheadings and searched for information about ISIS, it may not have moved on so quickly from its investigation into his activities. Experts have likewise noted an apparent gap in the "armory" of counterterrorism investigators.[23] But lowering the barriers to law enforcement access to private information raises a host of civil liberties concerns, both for those who seek out such information for personal purposes, and those who have research interests in the subject. The vanguard of terrorist threats calls upon us to reexamine the balance our legal system strikes between civil liberties and national security.

This Note proceeds in three Parts. Part I briefly describes how ISIS is breaking the mold of global terrorist groups (and the laws designed to combat them) by "inspiring" violent attacks in the United States. Part II then examines the current tools available to law enforcement and intelligence professionals for conducting surveillance of those who are drawn toward terrorist propaganda. It concludes that the current statutory framework likely does not allow for digital

19. Rukmini Callimachi, *What New York Attack Suspect's Words May Say About ISIS Ties*, N.Y. TIMES (Nov. 2, 2017), https://nyti.ms/2zbkEVg.

20. Rukmini Callimachi et al., *Islamic State Claims Responsibility for Lower Manhattan Terrorist Attack*, N.Y. TIMES (Nov. 2, 2017), https://nyti.ms/2z9sgaB. As of this writing, Saipov's potential direct connections to ISIS representatives remain under investigation. *Id.*

21. Missy Ryan, Adam Goldman, Abby Phillip & Julie Tate, *Both San Bernardino Attackers Pledged Allegiance to the Islamic State, Officials Say*, WASH. POST (Dec. 8, 2015), http://wapo.st/1OO4bJR?tid=ss_tw.

22. The federal government has reinforced the prominence of these attacks in public consciousness. Indeed, shortly after the Manhattan truck attack in October 2017, Attorney General Jeff Sessions publicly stated that "[t]he largest category of counterterrorism cases in the United States under investigation today are of people inspired by ISIS." Mark Moore & Carl Campanile, *Sessions: People Inspired by ISIS Represent Majority of Terror Probes*, N.Y. POST (Nov. 2, 2017), https://nypost.com/2017/11/02/sessions-people-inspired-by-isis-represent-majority-of-terror-probes.

23. Diane Webber, *Can We Find and Stop the "Jihad Janes"?*, 19 CARDOZO J. INT'L & COMP. L. 91, 121 (2011).

surveillance of individuals solely because they observe terrorist groups' content, if they have not also established relationships with terrorist groups or operatives. Finally, Part III explores the possibility of allowing such surveillance in light of the risks it would pose to core First Amendment values.[24] While the government's interest in detecting and disrupting terrorist threats is robust, whether the government's interest or the considerable individual interests at stake are weightier may be in the eye of the beholder.[25] In any event, this Note suggests that a regime allowing surveillance based on viewing terrorist propaganda would need to be scrupulously limited to pass First Amendment muster. Ultimately, the viability of expanded surveillance thus turns on the government's ability to take practical precautions to safeguard individuals' expressive freedoms—particularly in exploring Internet content for educational or research purposes.

I. "INSPIRED" ATTACKS IN THE ISIS ERA

ISIS is not the first international terrorist group to challenge existing law enforcement and intelligence paradigms. Although al-Qaida and other groups had targeted U.S. interests before September 11, 2001, the coordinated attacks launched on that day brought the threat of jihadist terrorism to the forefront of the national consciousness. 9/11 prompted much of the extant legal framework for detecting and disrupting terrorist threats, including the USA PATRIOT Act.[26]

Indeed, a devastating missed opportunity to prevent the 9/11 attacks illustrated the perceived need for lawmakers to close a gap in terrorism investigators' authority. It became clear after 9/11 that a man the FBI had detained in August 2001 had been a twentieth operative planned for

24. To be sure, expanded surveillance authorities allowing the government to monitor online activity based on the content individuals view online could be vulnerable to challenge on Fourth Amendment and Fourteenth Amendment grounds. This Note focuses only on the threat such a scheme might pose to First Amendment expressive freedoms.

25. *Cf.* Holder v. Humanitarian Law Project, 561 U.S. 1, 28 (2010) (acknowledging the government's interest in combatting terrorism as an "urgent objective of the highest order").

26. *Cf.* James McClintick, *Web-Surfing in Chilly Waters: How the Patriot Act's Amendments to the Pen Register Statute Burden Freedom of Inquiry*, 13 AM. U. J. GENDER SOC. POL'Y & L. 353, 360 (2005) ("Widespread public anxiety after the September 11 tragedies spurred Congress to grant some of the Justice Department's demands for enhanced surveillance capability."). The specter of 9/11 was also invoked to justify arguably illegal surveillance actions in its immediate aftermath. In 2005, after it came to light that the Executive Branch had engaged in a four-year, large-scale warrantless electronic surveillance program, President George W. Bush said in a press conference, "We know that a two-minute phone conversation between somebody linked to al-Qaeda here and an operative overseas could lead directly to the loss of thousands of lives. . . . I've reauthorized this program more than 30 times since the September 11th attacks, and I intend to do so for so long as our nation . . . faces the continuing threat of an enemy that wants to kill American citizens." Press Conference of the President (Dec. 19, 2005).

involvement in the attacks. But investigators hadn't had enough evidence linking him to al-Qaida to obtain a court order to search his laptop, and were unable to obtain any information from him about possible plots.[27] In December 2004, Congress amended the Foreign Intelligence Surveillance Act (FISA) to allow for electronic surveillance of individuals who could not fairly be categorized as "members" of international terrorist groups.[28] The statute was intended to encompass "lone wolves": anyone "acting in sympathy with the aims of a terrorist group but not on its behalf" or "perhaps acting on behalf of a terrorist group but in such a way that the requisite connection still could not be demonstrated."[29] The law broadened the reach of surveillance authorities beyond those who could be shown to be bona fide "members" of a terrorist group.[30]

ISIS is further challenging the scope of counterterrorism authorities. The group is ostensibly headquartered in Syria and Iraq, but it encompasses operational branches in several other countries.[31] ISIS also has a robust propaganda apparatus and social media presence; it is reported to have some 300 American or U.S.-based sympathizers active on social media,[32] and periodically produces an English-language magazine.[33] The group also has a habit of highlighting attacks carried out in its name, even if it had no role in planning them.[34] ISIS is thus "purposeful[ly] blurring . . . the line between operations that are planned and carried out by the terror group's core fighters and those carried out by its sympathizers."[35] And as the Pulse attack demonstrated, the group's activities frequently fall beyond investigators' reach.

---

27. Patricia Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 426 (2005).

28. *Id.* at 427.

29. *Id.*

30. The Senate Judiciary Committee's Report on the so-called "lone wolf" amendment explained that the change was necessary to confront the "increasingly . . . decentralized" nature of terrorist activity. S. REP. No. 108-40, at 3-4 (2003). The Committee explained that, in its view, "al-Qaida is far less a large organization than a facilitator, sometimes orchestrator of Islamic militants around the globe. These militants are linked by ideas and goals, not by organizational structure." *Id.* at 5.

31. *See* JAMES R. CLAPPER, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY BEFORE THE SENATE ARMED SERVICES COMMITTEE 5 (Feb. 9, 2016), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (mentioning ISIL affiliates based in Egypt and Libya, and the group's influence over Boko Haram in Nigeria).

32. LORENZO VIDINO & SEAMUS HUGHES, ISIS IN AMERICA: FROM RETWEETS TO RAQQA 21-22 (2015), https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf.

33. Bethan McKernan, *ISIS' New Magazine Rumiyah Shows the Terror Group is 'Struggling to Adjust to Losses'*, THE INDEPENDENT (Sept. 6, 2016), http://www.independent.co.uk/news/world/middle-east/isis-propaganda-terror-group-losses-syria-iraq-a7228286.html.

34. Brendan I. Koerner, *Why ISIS is Winning the Social Media War*, WIRED (Apr. 2016), https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat.

35. Callimachi, *supra* note 2.

If "lone wolves"—individuals acting with the guidance or blessing of a known terrorist group—presented a challenge to counterterrorism investigators and intelligence professionals, ISIS's model has redoubled that challenge. How can the United States prevent attacks that are merely "inspired" by terrorist groups' goals and tactics, but not directed by known terrorist actors? Is there any way for the FBI to identify individuals like Omar Mateen, Sayfullo Saipov, and the San Bernardino attackers before they take deadly action?

II. GAPS IN CURRENT SURVEILLANCE LAW

The legal tools currently available to law enforcement and intelligence professionals almost certainly preclude electronically monitoring an individual based solely on probable cause that the individual has viewed terrorist propaganda. Although in some cases this activity may foreshadow a resort to violence, the existing legal standards pose significant obstacles to using evidence of that activity to pursue additional electronic surveillance.

A. *Title III and Requisite Underlying "Alleged Criminal Offenses"*

Title III of the Omnibus Crime Control and Safe Streets Act of 1968[36] established requirements for law enforcement professionals seeking court orders to conduct electronic surveillance on suspected criminals. An application under Title III must contain detailed information about (1) the identity of the target, (2) the facilities and type of communication to be targeted, (3) the period of time for surveillance, (4) an alleged criminal offense, and (5) whether alternative investigative methods are unlikely to succeed or would be too dangerous.[37] Perhaps the strongest of the existing surveillance tools, a warrant obtained under Title III allows its bearer to obtain information about the fact that an electronic communication occurred as well as its content.[38]

Even if a Title III application contains all the requisite information, however, a judge will only issue a warrant for surveillance if she finds there is probable cause to believe that communications *related to a crime* will be obtained as a result.[39] Under that standard, if law enforcement is aware that an individual has viewed propaganda repeatedly, or submitted an inquiry to terrorist representatives, it may nonetheless be difficult to obtain a warrant to for additional electronic communications. As a threshold matter, viewing

36. Pub. L. No. 90-351, 82 Stat. 211 (codified as amended at 18 U.S.C. § 2510 et seq. (2016)).

37. 18 U.S.C. § 2518(1)(b)-(d) (2016).

38. 18 U.S.C. § 2510(4) (2016) (defining "intercept" as "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device).

39. 18 U.S.C. § 2518(3) (2016) (emphasis added).

terrorist propaganda online is not a crime.[40] Beyond viewing the material, if authorities are not sure "exactly what offense is planned" or "whether some unspecified offense is being committed or about to be committed, they will not be able to establish the probable cause required to obtain a warrant."[41] Although law enforcement may have a better case with a tip from an informant (as in the case of Omar Mateen), that evidence amounts only to probable cause that the individual has viewed the terrorist content; even if evidence indicating that a person is viewing such information is reliable, it may not create a sufficient connection to a potential *crime* to justify surveillance.

B. *Pen Registers and the "Ongoing Criminal Investigations" Requirement*

Historically distinct from Title III surveillance, the application to obtain surveillance via pen register has less stringent requirements. The information law enforcement can obtain from pen registers, however, is correspondingly limited.

Pen registers began as relatively rudimentary devices with "limited capabilities"; they were installed through the phone company, and could record the phone numbers calling into, or being dialed out from, a specific telephone line.[42] In the wake of 9/11, as part of the USA PATRIOT Act,[43] Congress expanded authorization for pen register "surveillance" to include analogous monitoring of online communications.[44] Under that statute, a court may authorize the placement of a pen register device if it is satisfied that the information likely to be obtained by the device is "relevant to an ongoing criminal investigation."[45]

For investigators, pen registers have an important drawback: The *content* of intercepted communications is off-limits. The statute itself admonishes authorities engaged in pen register surveillance to "restrict[] the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire and

---

40. *See infra* Part IV.A.iii. (discussing one scholar's proposal to criminalize such activity).

41. *See* Webber, *supra* note 23, at 121 (footnote omitted).

42. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (upholding the constitutionality of the use of a pen register without a warrant on the grounds that the defendant had no reasonable expectation of privacy in the phone numbers he dialed); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 570 (2009). By statute, law enforcement may not use pen register or "tap and trace" devices except with a court order obtained either under the statute regulating pen registers or FISA. 18 U.S.C. § 3123 (2016).

43. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

44. *See* 18 U.S.C. § 3127(3) (2016) (defining a pen register as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted").

45. *Id.* at § 3123(a)(1).

electronic communications *so as not to include the contents* of any wire or electronic communication."[46]

Although pen registers can only collect routing information, they could nonetheless be useful tools for disrupting the kinds of attacks with which this Note is primarily concerned. For the purposes of preventing so-called "inspired" terrorist attacks, discovering an individual's full browsing history, for example, or even the IP addresses of their correspondents, may provide useful clues to their activities and the potential threat they pose.

But the government still faces major obstacles to making even the lesser showing required to use pen registers to monitor individuals who view terrorist propaganda online. Under the pen register statute, the information sought must be "relevant to an ongoing criminal investigation."[47] As in the Article III context, it will be very difficult to link browsing activity to criminality. For example, the FBI's initial inquiry into Omar Mateen's activities was prompted by suspicions that he had links to terrorist groups; the investigation did not proceed on the theory that Mateen was a suspect in a particular crime.[48] It never amounted to an "ongoing criminal investigation." As proved true in his case, without external information indicating the suspect is involved in, or wanted in connection with, a specific crime, it would likely be impossible to obtain an order for a pen register recording an individual's browsing history.

C. *The Foreign Intelligence Surveillance Act and the "Agent of a Foreign Power" Standard*

The challenges that arise when authorities try to shoehorn terrorism investigations into the criminal model[49] counsel in favor of relying on a statute that is aimed specifically at gathering information for intelligence, rather than prosecution, purposes. FISA allows for electronic surveillance even without a connection to an ongoing criminal investigation. And despite its name, FISA authorizes such surveillance inside the United States.[50] A more potent tool than the pen register, FISA provides investigators with the ability to obtain "the

46. *Id.* at § 3121(c) (emphasis added). Interestingly, although section 3121 limits pen register collection to "dialing, routing, addressing, or signaling information" and explicitly excludes any content, some observers caution that Internet activity eludes clear distinctions between content and routing information. *See* James McClintick, *supra* note 26, at 361; *see also infra* Part IV.B.

47. 18 U.S.C. § 3123(a) (2016).

48. *See supra* notes 4-12 and accompanying text (discussing the FBI's initial investigation into Omar Mateen's suspected links to terrorist groups); *see also* Wilber, *supra* note 3 (explaining that agents had no "underlying crime" of which to suspect Mateen).

49. *Cf.* United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297, 314-17 (1972) (rejecting the government's attempt to create an exception to the warrant requirement for surveillance on "domestic security" interests).

50. 50 U.S.C. § 1803(a)(1) (granting the Foreign Intelligence Surveillance Court jurisdiction to hear and grant applications for intelligence-related surveillance "anywhere within the United States").

contents of any wire or radio communication sent by or intended to be received" by the suspect.[51] FISA thus appears the most promising for agents hoping to obtain information about the online activities of someone they know to be viewing terrorist propaganda online.

In order for a judge on the Foreign Intelligence Surveillance Court to grant a surveillance order, she must make a specific finding that there is probable cause to believe, among other things,[52] that "the target of the electronic surveillance is a foreign power or an agent of a foreign power."[53] The definition of "foreign power" includes any "group engaged in international terrorism or activities in preparation therefor."[54] Additionally, any non-U.S. person who "engages in international terrorism or activities in preparation therefor,"[55] or any U.S. person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power,"[56] can qualify as an "agent of a foreign power."

But despite casting a wide net around potential surveillance targets who have connections to international terrorist organizations, FISA's requirements generate grave doubt about the government's ability to obtain surveillance of the Internet activity of individuals (especially U.S. persons[57]) who could be "inspired" to commit terrorist attacks.

There are several potential obstacles to surveilling viewers of terrorist propaganda under FISA. First, until potential attackers have contacted bona fide terrorist representatives, it would be nearly impossible to establish a principal-agent relationship in the conventional sense between the group and the surveillance target. Even if an attacker started planning an operation with the concerted goal of promoting the group's agenda, it is not clear he would be acting "on behalf of" the group, if the group was totally unaware of his actions.

Even the more recently-adopted provisions of FISA specifically aimed at preventing "lone wolf" attacks do not fully encompass the kind of behavior that preceded Omar Mateen's attack on the Pulse nightclub. Before 9/11, FISA

---

51. *Id.* at § 1801(f)(1) (emphasis added).

52. *See id.* at § 1805.

53. *Id.* at § 1805(a)(2)(A).

54. *Id.* at § 1801(a)(4).

55. *Id.* at § 1801(b)(1)(C).

56. *Id.* at § 1801(b)(2).

57. *Id.* at § 1801(i) (defining "United States persons" to include citizens and lawful permanent residents). FISA is the only one of the three surveillance methods explored in this Note to set up different standards for U.S. persons and non-U.S. persons. Title III's operative provision refers only to the "person" targeted for surveillance. 18 U.S.C. § 2518. Pen register laws likewise specify only that applicants must state the identity of "the person" whose phone line will be targeted, and "the person" who is the subject of a criminal investigation, 18 U.S.C. § 3123(b)(1)(A)-(B), and authorization ultimately turns on the relevance of the "information likely to be obtained" by the device, 18 U.S.C. § 3132(a)(1)(2016). The statute provides that an order authorizing the use of a pen register "shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." *Id.*

limited its designation of "agents of a foreign power" to anyone who was "a member of or affiliated with" an international terrorist group.[58] In December 2004, Congress broadened its definition with respect to terrorist actors to the one the law reflects today, which encompasses any non-U.S. person who "engages in international terrorism or activities in preparation therefor."[59] "International terrorism," an admittedly ambiguous term, in turn is limited by FISA's text to activities that "occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum."[60] It is not entirely clear what work this provision does; If "inspired" attacks could be construed as transcending national boundaries via the media materials that brought the group or its ideology to the attacker's attention, nearly all acts of violence could be considered "international."[61] And while the missing twentieth 9/11 hijacker was fairly clearly engaged in an international operation, whether Omar Mateen, a U.S. citizen in Florida, also meets that definition is not nearly as obvious. Online propaganda and "inspired" attacks continue to test the limits of existing surveillance tools. The remainder of this Note considers ways the toolkit might be expanded to better address these threats.

III. FIRST AMENDMENT LIMITATIONS ON SURVEILLING VIEWERS OF TERRORIST PROPAGANDA

The prevalence of attacks by individuals who have absorbed terrorist propaganda but never coordinated with a terrorist group has prompted many observers—both in government[62] and in the academy[63]—to ask whether a new approach to counterterrorism is warranted. Indeed, days after the deadly October 2017 truck attack, Attorney General Jeff Sessions publicly lamented law enforcement's inability to independently obtain electronic evidence about potential terrorists and the government's dependence on the largesse of technology companies for information.[64]

---

58. Bellia, *supra* note 27, at 427.

59. *Id.* at 427-28; *see also* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (codified at 50 U.S.C. § 1801(b)(1)(C)(2016)).

60. 50 U.S.C. § 1801(c)(3).

61. *See, e.g.*, United States v. Duggan, 743 F.2d 59, 74 (2d Cir. 1984) (describing the rationale for adopting a rule that allows surveillance of terrorist actors in the United States, even when their activity is directed entirely outside the United States).

62. *See* Moore & Campanile, *supra* note 22.

63. *See, e.g.*, Eric Posner, *ISIS Gives Us No Choice but to Consider Limits on Speech*, SLATE (Dec. 15, 2015, 5:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.html.

64. Moore & Campanile, *supra* note 22.

Any expansion of the counterterrorism toolkit would be subject to a number of practical and legal constraints. This Note focuses on what such an expansion would mean for the First Amendment's protections for expressive freedoms. The remainder of the Note evaluates potential responses to "inspired attacks" based on the First Amendment erosion each response would cause. It seeks to provide a helpful framework for weighing the competing government and individual interests involved in counterterrorism policy and determining which possible responses are the most viable.

A. *Potential Responses to the Threat of Online Radicalization and "Inspired" Attacks*

1. *Removing the Content*

Perhaps the most obvious response to the rise in "inspired" attacks is to remove incendiary terrorist propaganda from wherever it is hosted on the Internet. Virtually all such material is hosted on websites and servers owned by private entities. As a result, those entities' efforts to remove content can generally avoid the constitutional constraints that bind government efforts to limit expression.[65] The flipside of that coin, however, is that law enforcement and intelligence investigators are limited by private companies' willingness to comply with government requests to take down content. Fortunately for the government, Twitter, Facebook, and other social media sites have often found it in their business interest to remove terrorist propaganda from their sites.[66]

---

65. *But see, e.g.*, United States v. Reed, 15 F.3d 928, 931-33 (9th Cir. 1994) (imposing Fourth Amendment requirements on a hotel manager's search of the defendant's room because "the government knew of and acquiesced in the intrusive conduct," and the manager "intended to assist law enforcement efforts."). Outside the United States, authorities sometimes have more direct authority to remove terrorist content hosted online. In the wake of the November 2015 Paris attacks, French lawmakers approved a proposal to give authorities additional leeway during a state of emergency to "block websites and social-media accounts that encourage or condone terrorism." Kaveh Waddell, *Shutting Down Jihadist Websites Won't Stop Terrorism*, ATLANTIC (Nov. 24, 2015), https://www.theatlantic.com/technology/archive/2015/11/free-speech-online-is-at-risk-after-paris-attacks/417411. U.S. politicians have also called for a more direct government role in dismantling terrorists' web presence. *See id.*

66. In April 2015, Twitter reported that it had suspended 10,000 ISIS-linked accounts. Waddell, *supra* note 65 (describing the move as "cutting out a chunk of the group's network, which is estimated to include between 50,000 and 90,000 accounts"). The most recent scholarship suggests, however, that private actors' willingness to comply may be diminishing. *See* Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 685 (2017) ("While companies like Yahoo, Facebook, and Twitter are able to carefully filter advertising content to their users, they choose not to eliminate messages of terrorist organizations using their servers."); Benjamin Good, *Google and Twitter Speak Up in Support of the First Amendment Rights of Their Users*, AM. CIVIL LIBERTIES UNION (Jan. 20, 2016, 2:45 PM), https://www.aclu.org/blog/free-future/google-and-twitter-speak-support-first-amendment-rights-their-users (recounting a recent case in which Google and Twitter

Unfortunately, the vastness of the Internet and sheer number of terrorist mouthpieces renders this strategy an exercise in law enforcement whack-a-mole: As soon as one account is deactivated, another can pop up in its place, making it "effectively impossible to silence a persistent voice online."[67] Even apart from any constitutional concerns it would present, removing content thus seems an unsustainable solution to the threat of "inspired" attacks.

2. *Prosecuting the "Speaker"*

Given the difficulty of removing individual pieces of propaganda posted online, the government could instead try to attack the problem at its source, and prosecute those individuals or groups who create and post the information. Prosecuting the "speaker" in this way might proceed under one of two theories: the propagandist may have illegally provided material support to terrorism "under the direction of, or in coordination with" a terrorist group,[68] or may have illegally incited violence.[69] These criminal prohibitions are fraught, of course, not least because they have been subject to their own constitutional challenges.[70] But setting aside potential arguments about the constitutionality of this approach, practical considerations again counsel against prioritizing prosecutions of terrorist propagandists. Many live outside the United States,[71] including in safe havens within the borders of hostile or unstable countries. And many are careful to conceal their identities while they browse the web,[72] a reality likely to frustrate prosecutors' efforts.

3. *Prosecuting the Viewer*

To more effectively counter the threat of individuals in the United States reading and acting upon terrorist propaganda, at least one scholar has advocated taking legislative action to penalize viewing terrorist groups' online materials. Professor Eric Posner has proposed a law that, among other things, would "make[] it a crime to access websites that glorify, express support for, or

---

filed amicus briefs in support of an online forum's request to keep its users' identities anonymous).

67. Waddell, *supra* note 65.

68. Holder v. Humanitarian Law Project, 561 U.S. 1, 26 (2010). For the various statutory formulations of this prohibition, see 18 U.S.C. §§ 2339A-2339B (2016).

69. *See, e.g.*, 18 U.S.C. § 2385 (2016) (criminalizing anyone who incites "overthrowing or destroying the government of the United States").

70. *See, e.g.*, *Holder*, 561 U.S. at 40 (affirming the constitutionality of a federal law criminalizing the provision of material support to terrorists); Brandenburg v. Ohio, 395 U.S. 444 (1969) (holding the prosecution of a Ku Klux Klan member under an Ohio law unconstitutional).

71. *But see* VIDINO & HUGHES, *supra* note 32, at 21(identifying some 300 American or U.S.-based sympathizers active on social media).

72. *See id.* (explaining that identifying ISIS influencers in the United States is difficult "because most online ISIS sympathizers seek anonymity").

provide encouragement for ISIS or support recruitment by ISIS."[73] Posner envisions enforcing the law through graduated penalties—including a mere "warning letter from the government" for first-time viewers—and calls for a broad exemption for research by journalists, academics, and security professionals.[74]

Posner acknowledges, as he must, that existing First Amendment case law precludes his preferred solution. Decades ago the Supreme Court in *Brandenburg v. Ohio*[75] set out the prevailing framework for evaluating government efforts to criminalize violence-related speech. Reversing the conviction of a Ku Klux Klan member charged under Ohio's criminal syndicalism statute, the Court in that case drew a distinction between "mere advocacy" of violence on the one hand, and incitement to violence on the other.[76] After *Brandenburg*, a government may only punish speech "where such advocacy is *directed* to inciting or producing *imminent lawless actions* and is *likely* to incite or produce such action."[77]

There is virtually no construction of the *Brandenburg* standard that would allow the States or the federal government to criminalize the viewing or reading of terrorist propaganda on the Internet. Even if the law could exclude innocuous observers such as journalists and academics, the very impulse to exclude those who view content without endorsing it is telling. After all, if journalists and academics who seek out terrorist propaganda cannot be said to endorse it, it becomes increasingly difficult to argue that anything about merely viewing the content constitutes "mere advocacy," much less incitement to violence. In addition, the requirement that citizens must disavow the content to avoid punishment—arguably necessary for them to fall under Posner's proposed exceptions—would effectively allow the government to stem the "flow of ideas" to citizens, a power the Supreme Court has resisted granting.[78]

4. *Using the Viewing of Terrorist Material as a Basis for Further Electronic Surveillance*

If criminalizing the viewing of terrorist propaganda is unlikely to survive constitutional scrutiny, perhaps a less aggressive, less invasive response to the threat of "inspired" attacks would pass muster. A final potential response to the threat that potential attackers like Omar Mateen pose is to authorize law enforcement officers to monitor individuals' Internet activities whenever there

---

73. Posner, *supra* note 63.

74. *Id.*

75. 395 U.S. 444 (1969).

76. *Id.* at 449.

77. *Id.* at 447 (emphasis added).

78. *See* Lamont v. Postmaster Gen., 381 U.S. 301, 306 (1965) (invalidating a statute that required postal workers to destroy communist propaganda traveling through the mail unless the addressee specifically requested delivery, on the grounds that it impinged addressees' First Amendment rights).

is probable cause to believe they have viewed terrorist propaganda online, even if they are not in communication with known terrorist operatives or groups. In light of the legal and practical barriers to prosecuting individuals who publish or view terrorist propaganda, there may be more promise in merely surveilling those who routinely view such material. Indeed, if law enforcement's goal is to prevent ideological affinity from materializing into violent action, monitoring viewers may meet authorities' needs.[79]

Although the existing statutory tools arguably do not authorize surveillance on this basis, there is some case law suggesting that Congress could enact law to authorize it. The Supreme Court long ago suggested that Title III's requirements might be relaxed in specific circumstances. In the *Keith* case, the Court indicated that a statute created for domestic security purposes could deviate from Title III in at least three ways. First, "the application and affidavit showing probable cause need not follow the exact requirements of [Title III] but should allege other circumstances more appropriate to domestic security cases." [80] Second, "the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court."[81] Finally, "the time and reporting requirements need not be so strict as those in [Title III]."[82] The remainder of this Part considers First Amendment barriers to devising such a statutory scheme to surveil online viewers of terrorist propaganda.

B. *First Amendment Evaluation of Expanding Surveillance Authority*

Courts have not hesitated to rigorously scrutinize government actions that risk curbing free speech, including those that fall short of prosecuting the speaker.[83] When the government takes actions that "inflict[] a palpable injury on the individual because of his lawful beliefs,"[84] it must justify them with a "paramount" or "vital" government interest.[85]

---

79. *See* Matthew Waybrecht, *Free Speech in an Era of Self-Radicalization*, LAWFARE (Feb. 26, 2016, 7:24 AM), https://www.lawfareblog.com/free-speech-era-self-radicalization ("The applicability of *Brandenburg* to the current fight against radical Islamic terrorism may also be moot to the extent that the government finds it more valuable to monitor "radicalizers" (and those who are following them) than to try to prosecute them, especially since so many are overseas.").

80. United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 323 (1972).

81. *Id.*

82. *Id.*

83. *See, e.g.*, Clark v. Library of Cong., 750 F.2d 89, 94 (D.C. Cir. 1984) ("Whether or not the government intended to punish or coerce the individual cannot be the sole test of legitimacy in such governmental action.").

84. *Id.* ("Where the government's action inflicts a palpable injury on the individual because of his lawful beliefs, it has the direct and consequent effect of chilling his rights to freedom of belief and association.").

85. Elrod v. Burns, 427 U.S. 347, 362 (1976). The case law also requires the government to show that its chosen course is the least restrictive means available to protect its interest. *Id.* at 362-63.

1. *Measuring the Government's Interest*

The question of whether the government has a sufficient interest in monitoring the online activity of individuals who view terrorist propaganda has not been extensively litigated in the courts. But similar questions have been posed by parties who suspect they might be subject to surveillance seeking prospective injunctive relief, and by those seeking damages for past unconstitutional surveillance, typically following a criminal prosecution. As the below examples demonstrate, these procedural pathways have made it difficult to isolate the measure of the government's interest in surveilling someone who is suspected of viewing terrorist messaging.[86]

Outside the terrorism context, courts have been hesitant to enjoin government surveillance in advance. In one case regarding planned FBI surveillance of a Young Socialist Alliance (YSA) convention, the Second Circuit vacated just such an injunction, citing separation-of-powers concerns.[87]

Damages actions for past unconstitutional surveillance also complicate the analysis of the government's interest in conducting surveillance. These kinds of suits can only be brought if individuals are aware that they have been surveilled. Because the government is unlikely to disclose the fact of surveillance except in the course of a criminal prosecution (or where disclosure is mandated by statute), it is difficult to discern how courts might weigh the government's interest in conducting this kind of surveillance apart from the information's utility in uncovering criminal activity.

As to the First Amendment, courts deciding each of these kinds of cases have employed pro-law enforcement standards. In evaluating motions to enjoin future surveillance, courts have purported to apply something like heightened scrutiny, but have drawn the government's interest in surveillance broadly.[88] For example, in the district court's ruling in *Socialist Workers Party*, the court asked whether the YSA and the programming at its convention had "any relation to violence [or] illegal activity of any kind."[89] Despite this somewhat

86. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (reversing a lower court's grant of relief to various organizations who feared they might be subject to surveillance, on the grounds that they had not alleged sufficient facts to show injury and obtain standing to sue); Laird v. Tatum, 408 U.S. 1, 15 (1972) ("Carried to its logical end, this approach would have the federal courts as virtually continuing monitors of the wisdom and soundness of Executive action; such a role . . . is not the role of the judiciary, absent actual present or immediately threatened injury resulting from unlawful governmental action."); *see also* McClintick, *supra* note 26, at 373 ("[T]he question of what constitutes a justiciable First Amendment injury remains unsettled.").

87. Socialist Workers Party v. Att'y Gen., 510 F.2d 253, 255 (2d Cir. 1974) ("At first blush there would hardly seem to be a role less appropriate for or capable of effective performance by the federal judiciary than advance supervision of the investigative methods of the FBI on a case-by-case basis, particularly in the field of national security.").

88. *See, e.g.*, Socialist Workers Party v. Att'y Gen., 387 F. Supp. 747, 752 (S.D.N.Y. 1974) (asking whether the government has a "sufficiently compelling interest" to justify inhibiting the subjects' freedom of association).

89. *Id.* at 752.

broad requirement, however, the district court ruled against the government. After evaluating the YSA's parent organization's materials and finding its "current non-violent beliefs and . . . disavowal of violence" credible, the district court held that the FBI had "shown nothing in the way of a loss to its interests" that would result from granting the injunction.[90]

The Second Circuit partially vacated the injunction, however, leaving in place only the requirement that the FBI not share the names of convention participants with the Civil Service Commission.[91] The court explained that "[t]he FBI has a right, indeed a duty, to keep itself informed with respect to the possible commission of crimes; it is not obliged to wear blinders until it may be too late for prevention."[92] The Second Circuit thus drew the government's interest even more broadly than the district court had. But the Second Circuit's explanation does not fully probe the extent of that interest; the "duty" to prevent crime is, of course, not sufficient to justify any and all surveillance.[93] And procedurally, the Second Circuit appears to have rested its decision in part on the fact that the plaintiffs sought immediate injunctive relief,[94] suggesting it may not have been as dismissive of the plaintiffs' concerns if they had shown they had actually been subject to unwarranted surveillance.

The District Court for the Northern District of Illinois explored the limitations of a similar public-safety rationale in *Alliance to End Repression v. City of Chicago*.[95] There, the Chicago Police Department had used a number of tactics, including filming and photography, to surveil the undisputedly lawful activities of activists. The plaintiffs alleged that the Department's activities "chilled their exercise of first amendment rights."[96] Once again, the court referred to a capacious government interest in threat prevention. In evaluating the government's interest in monitoring the plaintiffs' activities, the court recognized that "even in the absence of a reasonable suspicion of criminal activity, the government has an interest in investigating civilian conduct so that it may determine whether some further action is needed to protect the public from criminal behavior."[97] That interest, however, did not entitle the

90. *Id.* at 753-54.

91. *Socialist Workers Party*, 510 F.2d at 257. The Commission had been known to use similar lists to question prospective federal employees. *Id.* at 254.

92. *Id.* at 256.

93. *See* Maryland v. King, 569 U.S. 435, 482 (2013) (Scalia, J., dissenting) (observing that while a decision authorizing police to take arrestees' DNA as routine booking procedure "will, to be sure, have the beneficial effect of solving more crimes[,] . . . so would the taking of DNA samples from anyone who flies on an airplane[,] . . . applies for a driver's license, or attends a public school").

94. *See Socialist Workers Party*, 510 F.2d at 256 (explaining that a court's decision as to "whether the conduct sought to be protected is a legitimate area for [government] investigation" ought to be made with the aid of "a full record and with ample time for reflection. . . .").

95. 627 F. Supp. 1044 (N.D. Ill. 1985).

96. *Id.* at 1047.

97. *Id.* at 1055.

Department to engage in any and all monitoring activities. The court suggested that, in light of the Department's interest in learning about threats to public safety, it may have been permissible for it to send agents to "open meetings to observe and record events."[98] But the Department's invasive actions were a bridge too far: Infiltrating an activist organization's private meetings did not constitute the "least drastic means" of obtaining enough information to keep apprised of potential future criminal behavior.[99]

Compared to its interest in attending private activist meetings, the government's interest in monitoring the Internet activity of those who view terrorist propaganda appears just as compelling. The government has an interest in preventing violent attacks—the likes of those it has witnessed multiple times in the past year—and surveilling the viewers of terrorist propaganda is one possible means of working toward that goal. In at least some cases, if the government has probable cause to believe an individual has been "radicalized" online[100] but does not display any outward affiliation with or affinity for a terrorist group, it could monitor their activity for any indication they intended to act on their convictions (for example, by discovering emails indicative of weapons purchases or casing targets). These indications, in turn, might help investigators disrupt future violent actions.

2. *Accounting for Individual Freedoms*

Assuming the government's interest in obtaining information about those who view terrorist propaganda online is sufficiently compelling, is there any way for the government to capture that information without gutting individuals' freedoms of speech and association? Is there a "least drastic means" of preventing "inspired" attacks before they occur?

Allowing the government to know who is visiting terrorist websites, and to discover the further activity of visitors to those websites, would certainty curtail First Amendment expressive activity. Even short of criminalizing speech, the simple knowledge that "the Government may be watching chills associational and expressive freedoms."[101] This concern is perhaps most acute when it comes to the impact of government surveillance on truly "innocent" viewers—

98. *Id.* Of course, the City "[did] not simply send informers and infiltrators" to do just that; it secretly dispatched personnel into private meetings as well. *Id.*

99. *Id.* ("The court cannot find, and the City does not proffer, a compelling reason for permitting this sort of disruptive infiltration in the absence of any reasonable suspicion of criminal conduct.").

100. The subjective question of whether someone is "radicalized" may stretch the already flexible probable cause standard. *Cf.* Draper v. United States, 358 U.S. 307, 313 (1959) ("In dealing with probable cause . . . we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." (quoting Brinegar v. United States, 338 U.S. 160, 175 (1940))). Investigators might point to frequent participation in forums discussing extremist activities, or perhaps (as in Mateen's case), a tip from a witness.

101. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

that is, individuals who would view terrorist materials for some academic or research purpose rather than out of any genuine curiosity or affinity.

Observers have recognized the danger that broadening online surveillance authorities would chill academic freedoms. In 2005, James McClintick critiqued the broadening of pen register statutes to encompass Internet monitoring.[102] Beginning from the proposition that the First Amendment protects the right to conduct Internet research,[103] McClintick argues that a "legally actionable injury can result from a system of ongoing surveillance that creates nothing more than the mere possibility of a First Amendment burden."[104] Allowing authorities to monitor the Internet activity of anyone who visits a terrorist website could very well cause "even an innocent person" to fear that "investigators will, at some future date, interpret the fruits of their surveillance as evidence of terrorism or other forms of criminal activity."[105]

Any expansion of surveillance authority would need to use every possible means to avoid surveilling academics and journalists.[106] The harm that society would suffer if journalists and academics were forced to think twice before using the Internet to research terrorist messaging should not be underestimated. News investigations and academic publications are critical to keeping the public informed about the threat terrorists pose at home and abroad, and understanding the threat is critical to evaluating the legitimacy of our government's responses (including any efforts to prevent attacks using surveillance). Precautions might include minimization requirements like those found in the FISA statute;[107] the use of pen register-like devices to allow only "source and destination information," such as IP addresses, to be collected;[108] a threshold number of times that a visitor would need to be detected on a site to trigger further monitoring; or a robust preliminary review mechanism to weed out academics or researchers. Any efforts to assuage researchers' concerns that they might be subject to surveillance while conducting valuable research would be welcome. It remains unclear, however, that these mechanisms could adequately avoid the chilling effect that comes with monitoring. Even a minimally invasive procedure—perhaps requiring researchers to provide the government notice of their plans to view the content—involves an element of self-censorship the First Amendment likely does not tolerate.

---

102. McClintick, *supra* note 26, at 367-72 (arguing that the indiscriminate collection chills scholarly research).

103. *Id.* at 362 (citing Reno v. ACLU, 521 U.S. 844 (1997)).

104. *Id.* at 373.

105. *Id.* at 374. For a discussion of the analogous chill on associational freedoms that would result from unbridled locational monitoring, see Gerald J. Votava III, *First Amendment Concerns in Governmental Acquisition and Analysis of Mobile Device Location Data*, 13 U. PITT. J. TECH. L. & POL'Y 1, 9-10 (2013).

106. *Cf.* Posner, *supra* note 63.

107. 50 U.S.C. § 1801(h) (2016).

108. McClintick, *supra* note 26, at 377.

A separate set of concerns arises regarding the First Amendment interests of those who view terrorist propaganda because they sympathize with, or identify as members of, terrorist groups. As Professor Alexander Tsesis observes, "[s]upporters of terrorism communicate to advance violent political ideologies, which are typically protected by the First Amendment."[109] And the Supreme Court has made clear that readers and viewers enjoy First Amendment protection just as speakers do.[110] Surveillance would curb the associational and expressive activities of these viewers, whose online engagement is undisputedly lawful insofar as it does not amount to incitement. Tsesis is somewhat dismissive of these concerns. He writes, "The limited social value of terrorist speech, for such things as information acquisition or self-expression, is outweighed by the public interest to preserve safety and order."[111] But even setting aside the fact that Tsesis's focus is on the *producers* of terrorist propaganda rather than the viewers, it is not a foregone conclusion that the First Amendment rights of those who engage in such advocacy are trivial.[112] Indeed, the Supreme Court has subjected to strict scrutiny content-based limitations on otherwise lawful speech that helps terrorist groups.[113] And for good reason: Using government resources to crowd out even these arguably abhorrent views would be detrimental to the marketplace of ideas and political discourse.[114] Perhaps worse, sending the message that the government is suppressing sympathizers' expression may drive them further away from the mainstream, possibly toward violence.

Ultimately, however, a court might conclude that this concern, while non-trivial, must yield in a particularly acute threat environment. To be sure, one of the common threads in prior case law prohibiting government surveillance of radical groups was an unwillingness to place unique limits on a group's

109. Tsesis, *supra* note 66, at 653.

110. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) ("A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more."); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 756 (1976) ("Freedom of speech presupposes a willing speaker. But where a speaker exists . . . the protection afforded is to the communication, to its source and to its recipients both." (footnote omitted)); *see also* Reno v. ACLU, 521 U.S. 844 (1997).

111. Tsesis, *supra* note 66, at 701.

112. *Cf.* Brandenberg v. Ohio, 395 U.S. 444, 448 n.4 (1969) ("The right of peaceable assembly is a right cognate to those of free speech and free press and is equally fundamental." (quoting DeJonge v. Oregon, 299 U.S. 353, 364 (1937))).

113. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 27-28 (2010) (rejecting the government's argument that a material-support prosecution predicated on a humanitarian organization's speech to designated terrorist groups should be subject to intermediate scrutiny, and instead applying "a more demanding standard").

114. *Cf.* Aziz Z. Huq, *Preserving Political Speech from Ourselves and Others*, 112 COLUM. L. REV. SIDEBAR 16, 22 (2012) (describing how enforcement of the material support ban "changes the content and structure of the national political marketplace").

constitutional rights just because their ideas were unpopular.[115] The desire of present-day terrorist groups to disrupt the political order of the West parallels the revolutionary inclinations of some radical groups during the mid-twentieth century. But unlike the YSA, ISIS publicly praises the fatal attacks its followers carry out, the vast majority of which are directed against innocent civilians rather than the government.

Moreover, while it is easy to envision a socialist adherent who favors the dissolution of capitalism as we know it but does not believe that dissolution will come about in our era, the population of ISIS supporters who feel the group's goals are not worth working toward at this time is likely relatively small. Although concern for the marketplace of ideas is valid, the interests of those genuinely engaged in this type of association may not always outweigh the interest in preventing terrorist attacks, at least where ISIS has demonstrated an ongoing will and ability to "inspire" attacks within the United States.

Separate from individuals' expressive and associational freedoms that might be curbed by surveilling those who view terrorist propaganda, broadening surveillance authority creates the risk that the government might abuse its newfound authority. Professor Wadie Said has argued in the material-support context that the system places too much power in the hands of the Executive Branch. The enforcement of material support prohibitions, he argues, grants the State Department and the rest of the foreign policy establishment "seemingly limitless" authority to define "what constitutes terrorist activity."[116] Professor Said's concerns are well-placed, given that counterterrorism is largely an Executive Branch exercise. In the surveillance context, then, proper checks would need to be built into authorizing statutes to prevent the government from pursuing surveillance of groups simply because their views are unpopular. These checks could come in the form of specific enumeration of the organizations whose materials would be subject to surveillance, or a more robust legislative and public input on the formation of the State Department's list of designated terrorist organizations.

Relatedly, even if surveillance could be crafted to preserve First Amendment freedoms, it is worth pausing to ask why this particular kind of incendiary material—propaganda associated with ISIS, al-Qaida, or their affiliate groups—warrants surveilling at such a systemic level, while other materials do not. Several recent violent attacks were carried out by individuals driven to violence by other radical ideas they had absorbed from the Internet. In 2014, twenty-two-year-old Elliot Rodger killed six college students in Isla Vista, California, including three he shot to death in a sorority house. Rodgers was a regular on so-called "men's rights" websites, which advocate traditional

115. *See, e.g.*, Socialist Workers Party v. Att'y Gen. of the U.S., 387 F. Supp. 747, 752 (S.D.N.Y. 1974).

116. Wadie E. Said, *The Material Support Prosecution and Foreign Policy*, 86 IND. L.J. 543, 571-72 (2011).

gender roles and encourage men to engage in uber-masculine behavior.[117] In June 2015, Dylann Roof, a twenty-one-year-old white man, opened fire during Bible study at an African-American church in Charleston, South Carolina, killing nine people. Roof had created a website on which he posted exhortations of racial segregation, photos of himself with a Confederate flag, and descriptions of crimes committed by African-Americans, which were pulled from the site of a white nationalist group.[118] And in August 2017, James Alex Fields, Jr., a twenty-year-old white man, killed a woman when he drove his car through a crowd of protesters rallying against an assembly of white supremacists in Charlottesville, Virginia.[119]

With the rise of ISIS-"inspired" attacks, the present-day threat of jihadist terrorism increasingly mirrors mass shootings and other violence carried out in the name of different, destructive causes.[120] Indeed, government officials have observed "those under surveillance in the United States for possible ties to [ISIS] usually have little terrorism expertise or outside support, which makes thwarting an Islamic State-inspired attack less like stopping a traditional act of terrorism and more like trying to prevent a shooting at a school or movie theater."[121] Omar Mateen's motives for killing forty-nine people likewise must be acknowledged as complex; authorities reported that he may have attended Pulse nightclub as a regular and visited gay-interest chatrooms.[122] It may be that as the distinctions between the tactics involved in these kinds of attacks begin to dissolve, courts will be called upon to allow surveillance not only of those who view materials advocating attacks in the name of jihad, but also anyone who watches any manner of incendiary, violent, ideological material. The obvious concern is that allowing surveillance of potential ISIS sympathizers is the first step down a slippery slope of policing speech.

By the same token, the ubiquity of shootings carried out in the name of toxic ideology, and the Internet's role in disseminating all manner of unpalatable ideas, make it increasingly difficult to articulate a non-suspect

---

117. *See* Caitlin Dewey, *Inside the 'Manosophere' that Inspired Santa Barbara Shooter Elliot Rodger*, WASH. POST (May 27, 2014), http://wapo.st/TRkmx5?tid=ss_mail.

118. *See* Frances Robles & Nikita Stewart, *Dylann Roof's Past Reveals Trouble at Home and School*, N.Y. TIMES (July 16, 2015), https://nyti.ms/2jM6mBV.

119. Joe Ruiz, *Ohio Man Charged with Murder in Fatal Car Attack On Anti-White Nationalist March*, NPR (Aug. 13, 2017, 7:30 AM ET), https://n.pr/2uzyykV.

120. Indeed, the question of whether to label such mass shootings "terrorism" has sparked widespread debate. *Compare* Philip Bump, *Why We Shouldn't Call Dylann Roof a Terrorist*, WASH. POST (June 19, 2015), http://wapo.st/1GnzQZU?tid=ss_tw, *with* Rick Gladstone, *Many Ask, Why Not Call Church Shooting Terrorism?*, N.Y. TIMES (June 18, 2015), https://nyti.ms/2onDN2f.

121. Mazzetti, Lichtblau & Blinder, *supra* note 1.

122. Evan Perez, Shimon Prokupecz & Holly Yan, *Omar Mateen Scouted Disney Complex, Pulse, Official Says*, CNN (June 15, 2016, 12:25 AM), http://www.cnn.com/2016/06/14/us/orlando-shooter-omar-mateen; Mazzetti, Lichtblau & Blinder, *supra* note 1 (describing investigators' task of determining "how much the killings were the act of a deeply disturbed man . . . and how much he was driven by religious or political ideology").

reason why the religious material Omar Mateen viewed made him a more viable surveillance target than someone who conducted a similarly horrific mass shooting out of homophobic or racist animus.

There is thus a colorable argument to be made that the government's interest in discovering the electronic paper trail of individuals who view terrorist media online is simply not "paramount." While arguably more immediate than the threat posed by communist and socialist groups, the threat of ISIS-"inspired" attacks being carried out in the United States is not necessarily more grave than the threat of horrific crimes being carried out in the name of other invidious ideologies. However, the idea that terrorism stands apart from other crimes dominates the common consciousness, as well as legal discussions,[123] suggesting there may be some heightened government interest in preventing terrorist attacks over and beyond the interest in preventing crimes.

When determining whether and how to allow the government to surveil those who view terrorist propaganda on the Internet, balancing the government's interest in preventing atrocities against the risks to First Amendment freedoms and the marketplace of ideas does not yield a clear winner. The inquiry implicates bedrock questions about our society's values: the amount of risk we are comfortable assuming, and the amount of power we are comfortable placing in the government's hands. But if our society values security enough to go down this path, properly understanding the various interests at stake illuminates measures the government would need to take to tailor any future efforts and minimize the risk to First Amendment freedoms.

CONCLUSION

The rise of social media has provided terrorist groups with a platform from which to spread their ideas, gain followers, and attract recruits. It has allowed them to prompt violent action without even making contact with operatives, much less dispatching operational instructions. Instead, as was the case in the tragic attack on Orlando's Pulse nightclub, individuals can get the inspiration—and the resolve—to carry out a violent attack simply by watching videos and reading articles online. And because the existing legal tools likely do not allow for surveillance of individuals who merely view this information online, authorities may never learn of attackers' plans before they carry them out.

This novel and evolving threat suggests it may be time to reexamine existing surveillance powers and the doctrines they rest on. But any move to broaden surveillance authority will need to balance the government's considerable interest in preventing future "inspired" attacks with a compelling individual and societal interest in protecting the First Amendment rights of all those who browse the Internet. As this Note has discussed, the case law directly

123. For an examination of the idea of "terrorist exceptionalism" in the context of criminal prosecutions, see WADIE E. SAID, CRIMES OF TERROR 1-9 (2015).

addressing the First Amendment damage caused by the knowledge that one is being surveilled is sparse; still, it may be possible to craft a solution that contains sufficient protective measures to avoid drastically harming freedoms of speech and association.

Determining the best balance of government and individual rights depends on how we answer fundamental questions, including about how much our society is willing to tolerate a sincerely held—but never acted upon—set of beliefs endorsing violence. The Supreme Court's incitement jurisprudence seems to indicate that incendiary beliefs are perfectly permissible, as long as they do not demand immediate violent action. Indeed, our society tolerates such incendiary beliefs (white supremacy, for example) in moderate doses, and will legally protect those who express them. Ultimately, the equal-protection implications of increased surveillance of those who view terrorist propaganda are beyond the scope of this Note. But as the focus of counterterrorism investigators increasingly turns toward attacks committed by individuals acting alone, driven by an ideology that endorses hateful violence, new justifications will be needed to continue to single out this ideology from all the others that "inspire" individuals to attack.