HOLDING SOCIAL MEDIA PROVIDERS LIABLE FOR ACTS OF DOMESTIC TERRORISM

Chloe Berryman[*]

Abstract

Would the availability of a federal cause of action for domestic terrorism increase the risk of social media providers being held liable for facilitating domestic terrorism? Recently, there have been discussions concerning the role social media plays in acts of domestic terrorism. Many acts of domestic terrorism have been linked to the perpetrator's involvement with online groups who harbor similar goals.

There are several legislative obstacles to successfully suing a social media provider for aiding an act of domestic terrorism. One obstacle is the Antiterrorism Act of 1990 (ATA), which provides a civil remedy for international terrorism but not domestic terrorism. There has been increased discussion about the federal government's disparate treatment of domestic and foreign terrorism, with many scholars calling for the federal government to treat these acts equally. Another obstacle is the Communications Decency Act of 1996 (CDA), which shields social media providers from liability for content they did not create. Recent discussions and court decisions have indicated that changes to both the ATA and the CDA may be coming. If these threshold barriers were removed, the number of claims brought under the ATA would likely increase.

Victims may attempt to sue social media providers for aiding domestic terrorism, but one of the biggest obstacles to a successful claim is proving proximate cause. This Note discusses the scientific basis for the connection between social media use and acts of domestic terrorism and analyzes whether this connection is strong enough to prove causation on the part of the social media provider.

---

* J.D. Candidate 2021, University of Florida Levin College of Law; B.S. 2014, University of Central Florida. I would like to thank my mother, Sophia Reinhard, for her constant support and encouragement, and my brother, Gavin Berryman, for his comedic presence (on-campus and off). I would also like to thank my friends and colleagues on the *Florida Law Review* for making this Note possible.

INTRODUCTION

Domestic terrorism is classified as violent threats or acts "in furtherance of political or social objectives" that occur entirely within the United States and without foreign direction.[1] Over the past several years, acts of domestic terrorism have been on the rise, turning national attention to a discussion on domestic terrorism.[2] Despite this increase, there is limited recourse for victims of domestic terrorism and little legislation in place to deter these acts.[3]

Victims of domestic terrorism who bring suit face several obstacles. Federal laws concerning domestic terrorism do not match those concerning international terrorism.[4] Indeed, the Antiterrorism Act of 1990 (ATA)[5] provides a civil remedy for international terrorism.[6]

1. COUNTERTERRORISM DIV., FED. BUREAU OF INVESTIGATION, TERRORISM 2002–2005, at v (2007).

2. DEP'T OF HOMELAND SEC., STRATEGIC FRAMEWORK FOR COUNTERING TERRORISM AND TARGETED VIOLENCE 10 (2019) ("Domestic terrorists . . . have caused more deaths in the United States in recent years than have terrorists connected to [Foreign Terrorist Organizations]."); *see* Shirin Sinnar, *Separate and Unequal: The Law of "Domestic" and "International" Terrorism*, 117 MICH. L. REV. 1333, 1341 (2019).

3. *See* Katie Dilts, Comment, *One of These Things Is Not Like the Other: Federal Law's Inconsistent Treatment of Domestic and International Terrorism*, 50 U. PAC. L. REV. 711, 728 (2019).

4. *Id.* at 727.

5. Pub. L. No. 101-519, § 132, 104 Stat. 2250 (codified as amended at 18 U.S.C. §§ 2331, 2333–38 (2018)).

6. 18 U.S.C. § 2333(a).

Although the ATA provides some recourse, this remedy is not available for victims of domestic terrorism.[7]

Regardless of whether an attack is categorized as domestic or international terrorism, victims do not have an easy target from which to recover damages.[8] Recently, there have been discussions concerning the role social media plays in acts of domestic terrorism.[9] Many acts of domestic terrorism have been linked to the perpetrator's involvement with online groups with similar goals.[10] Under the ATA, victims may recover from secondary actors who aid and abet international terrorism.[11] Social media providers have become popular secondary actors to target but are shielded from liability by the Communications Decency Act of 1996 (CDA).[12]

As a result of these obstacles, successfully suing a social media provider for aiding and abetting an act of domestic terrorism is nearly impossible.[13] With the increase in domestic terror attacks, there has been renewed discussion surrounding these legislative obstacles, and change is on the horizon.[14] On the one hand, there has been increased dialogue about the federal government's disparate treatment of domestic and foreign terrorism, with many scholars calling for the federal government to treat these acts equally.[15] On the other, recent discussion surrounding

7. *Id.*; Dilts, *supra* note 3, at 728.

8. *See* Jimmy Gurulé, *Holding Banks Liable Under the Anti-Terrorism Act for Providing Financial Services to Terrorists: An Ineffective Legal Remedy in Need of Reform*, 41 J. LEGIS. 184, 222 (2015).

9. *See* JEROME P. BJELOPERA, CONG. RESEARCH SERV., R44921, DOMESTIC TERRORISM: AN OVERVIEW 48 (2017) (discussing social media and Internet use by domestic terrorists); Nele Schils & Lieven Pauwels, Ghent University, Address at the European Society of Criminology 2013 Conference: Explaining Violent Extremism: The Role of New Social Media (Sept. 2013), http://hdl.handle.net/1854/LU-4147823 [https://perma.cc/7S5P-A2ZL] (discussing growing concerns that "(self)radicalization and recruitment for violent extremism will rise under influence of the internet").

10. Emily B. Tate, Note, *"Maybe Someone Dies": The Dilemma of Domestic Terrorism and Internet Edge Provider Liability*, 60 B.C. L. REV. 1731, 1734–35 (2019).

11. *See* discussion *infra* Part I.

12. Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C. §§ 230, 560–61 (2018)); *see* 47 U.S.C. § 230(c)(1) (shielding social media providers from content they did not create).

13. Tate, *supra* note 10, at 1755.

14. *See id.* at 1747 (describing the increase in domestic terrorism); Barbara McQuade, *Proposed Bills Would Help Combat Domestic Terrorism*, LAWFARE BLOG (Aug. 20, 2019, 8:49 AM), https://www.lawfareblog.com/proposed-bills-would-help-combat-domestic-terrorism [https://perma.cc/Q52B-4WB7] (discussing proposed legislative changes).

15. *See, e.g.*, Dilts, *supra* note 3, at 734.

the CDA indicates that commentators are beginning to disfavor the blanket immunity granted to Internet Service Providers (ISPs).[16]

Would the availability of a federal cause of action for domestic terrorism increase the risk of social media providers being held liable for facilitating domestic terrorism? Even if the legislative obstacles were cleared, one of the highest hurdles to a successful claim is proving proximate cause.[17] This Note discusses the merits of providing a path to sue social media providers for aiding acts of domestic terrorism. It also discusses the scientific basis for the connection between social media use and acts of domestic terrorism and analyzes whether this connection is strong enough to prove proximate causation on the part of the social media provider.

I. THE ANTITERRORISM ACT (ATA)

The ATA provides a civil cause of action for any U.S. national injured by an act of international terrorism.[18] Several federal laws treat international and domestic terrorism very differently.[19] The ATA is no different; the right of action provided by the ATA does not extend to victims of domestic terrorism, leaving victims with no recourse under the statute.[20]

Acts of domestic terrorism "occur primarily within the territorial jurisdiction of the United States."[21] Conversely, international terrorism involves acts that "occur primarily outside the territorial jurisdiction of the United States" or acts that otherwise transcend national boundaries with regard to the population targeted by the acts, the location of the perpetrators, and the means employed by the perpetrators.[22]

16. *See* Jaime M. Freilich, Note, *Section 230's Liability Shield in the Age of Online Terrorist Recruitment*, 83 BROOK. L. REV. 675, 696 (2018) (advocating for an amendment to the CDA to allow liability for acts of terrorism); Michelle Roter, Note, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1382 (2017) (arguing that ISPs should have a duty to remove posts that incite terrorism).

17. *See* Ronbert H. Schwartz, Comment, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*, 48 LOY. U. CHI. L.J. 1181, 1202 (2017).

18. Gurulé, *supra* note 8, at 192.

19. Dilts, *supra* note 3, at 727 (discussing how federal terrorism law tends to exclude domestic terrorism).

20. *See* 18 U.S.C. § 2333(a) (2018).

21. Seth N. Stratton, Note, *Taking Terrorists to Court: A Practical Evaluation of Civil Suits Against Terrorists Under the Anti-Terrorism Act*, 9 SUFFOLK J. TRIAL & APP. ADVOC. 27, 41 (2004) (quoting Smith v. Islamic Emirate of Afg., 262 F. Supp. 2d 217, 221 (S.D.N.Y.), *amended*, No. 01 CIV.10132(HB), 2003 WL 23324214 (S.D.N.Y. May 19, 2003)).

22. *Id.* (quoting *Smith*, 262 F. Supp. 2d at 222).

Regardless of whether the terrorist act is domestic or international, another obstacle victims encounter is that there is no easy target to collect damages from. In other words, foreign terrorist organizations are unlikely to have assets plaintiffs can collect against.[23] Thus, plaintiffs file a majority of ATA lawsuits against secondary actors who provide material support to terrorists.[24]

Most ATA claims against secondary actors are unsuccessful,[25] particularly in jurisdictions that do not recognize aiding and abetting liability under the ATA.[26] The ATA's civil liability provision is silent on whether aiding and abetting creates a cause of action.[27] Separate ATA provisions "criminalize the provision of material support to terrorists in any form."[28] Section 2339A criminalizes the intentional or knowing support of a specific act of terrorism.[29] Section 2339B is broader, with criminal liability attaching when the defendant knowingly provides material support to a designated terrorist organization or an organization that the defendant knew was engaged in terrorism.[30] Under § 2339B, knowledge does not require "specific intent to further the organization's terrorist activities"; it refers to the secondary actor's knowledge of the aided organization's connection to terrorism.[31]

Recently, courts have construed violations of § 2339A or § 2339B as acts of international terrorism under § 2333.[32] This has allowed victims to bring civil lawsuits against secondary actors who provide material support to terrorists.[33] In addition to requiring the plaintiff to prove both the unlawful provision of material support and the requisite mental state, civil material-support claims require the plaintiff to prove causation.[34]

---

23. Gurulé, *supra* note 8, at 184.

24. *Id.*

25. *Id.*

26. *Id.* at 186.

27. *Id.* at 185; *see* 18 U.S.C. § 2333(a) (2018).

28. Anna Elisabeth Jayne Goodman, Comment, *When You Give a Terrorist a Twitter: Holding Social Media Companies Liable for Their Support of Terrorism*, 46 PEPP. L. REV. 147, 168 (2018); *see* 18 U.S.C. §§ 2339A–2339B (2018).

29. Rachel E. VanLandingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism, and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1, 29–30 (2017).

30. Emily Goldberg Knox, Note, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295, 304 (2014).

31. *Id.* at 306 (quoting Holder v. Humanitarian Law Project, 561 U.S. 1, 17 (2010)); VanLandingham, *supra* note 29, at 30. On the other hand, criminal prosecution has historically been directed at website hosts and founders that have radical websites rather than social media companies as a whole. *See* Knox, *supra* note 30, at 309.

32. CHARLES DOYLE, CONG. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. § 2339A AND § 2339B, at 12 (2016).

33. Goodman, *supra* note 28, at 169; *see* DOYLE, *supra* note 32, at 12.

34. Goodman, *supra* note 28, at 172.

Causation requires the plaintiff to prove that the provision of material support was the proximate cause of the injuries the plaintiff suffered in the attack.[35]

The definition of material support includes the provision of any tangible or intangible property or any service, including communications equipment.[36] Since the definition of material support is broad, the services social media platforms provide easily satisfy this element.[37]

II. SOCIAL MEDIA USE AND DOMESTIC TERRORISM

Following a terrorist attack, the most popular secondary actors to direct blame to are social media providers and other ISPs. It is well-established that the Internet has become an effective tool for terrorist organizations.[38] Terrorists can use the Internet to advance terrorist causes through "(1) Propaganda (including recruitment, incitement, and radicalization); (2) Financing; (3) Training; (4) Planning (including secret communication and open-source information); (5) Execution; and (6) Cyberattacks."[39] According to one commentator,

> [T]he Internet is an ideal platform for domestic and international terrorists because it affords easy access, minimal regulation and censorship, anonymity of communication, speed, low cost, a multimedia environment to combine text, graphics, audio, video and perhaps most significantly, the ability to shape coverage in the traditional mass media. Specifically, terrorists can bypass existing "selection thresholds" of traditional media to gain public attention by simply posting the controversial content themselves.[40]

One of the most discussed and researched ways that terrorists use social media to advance a terrorist agenda is through radicalization. Radicalization is the process of adopting an extremist worldview that

35. Tate, *supra* note 10, at 1745.

36. 18 U.S.C. §§ 2339A(b), 2339B(g)(4) (2018).

37. Goodman, *supra* note 28, at 172; *see* Nina I. Brown, *Fight Terror, Not Twitter: Insulating Social Media from Material Support Claims*, 37 LOY. L.A. ENT. L. REV. 1, 14 (2017).

38. DEP'T OF HOMELAND SEC., *supra* note 2, at 8 ("Communication advances have likely contributed to compressed 'flash-to-bang' timelines, the period between radicalization to violent extremism and mobilization to violence."); Zachary Leibowitz, Note, *Terror on Your Timeline: Criminalizing Terrorist Incitement on Social Media Through Doctrinal Shift*, 86 FORDHAM L. REV. 795, 811 (2017) ("Since terrorists' adoption of social media, there have been more frequent attacks and more threats of attacks than at any other period in time.").

39. Rodger A. Bates & Mara Mooney, *Psychological Operations and Terrorism: The Digital Domain*, J. PUB. & PROF. SOCIOLOGY, Feb. 2014, at 4.

40. *Id.* at 3.

"deems legitimate the use of violence as a method to effect societal or political change."[41] This process is usually gradual and involves "socialization into an . . . extremist belief system that sets the stage for . . . violence even if it does not make it inevitable."[42] Extremist groups may use social media to fully immerse potential recruits into their ideology.[43] During this process, the recruit's normal existence is diminished and replaced with an "alternate interpretation of reality."[44] Terrorist organizations accomplish this through the near constant production and transmission of violence and propaganda.[45]

A variety of processes converge to produce extremist behaviors and beliefs.[46] These include "grievances, networks, ideologies, and enabling environments and support structures."[47] Terrorist organizations typically use social media to "target[] disenfranchised youth with convoluted, fictional information and creat[e] grassroots terrorists within the U.S. borders."[48] This "[v]irtual mobilization isolates the individual from external societal controls and may foster a lack of accountability coupled with a cult mentality."[49] These tactics make it easier for terrorist organizations to push their extremist ideologies, which "provide a psychological mechanism of externalization, which [in turn] allows individuals to channel their personal frustrations and anger, and project blames onto other members of society."[50]

Individuals with existing personal or group grievances or mental illnesses may be easy targets for radicalization.[51] Personal grievances may include "economic marginalization and cultural alienation" and a "deeply held sense of victimization," as well as personal crisis.[52] Group grievances are grievances held "against a social group such as supporters of the democratic party, religious groups, minority groups, and

41. Mohammed Hafez & Creighton Mullins, *The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism*, 38 STUD. CONFLICT & TERRORISM 958, 960 (2015).

42. *Id.*

43. J.M. Berger, *The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion*, PERSPECTIVES ON TERRORISM, Aug. 2015, at 61, 62.

44. *Id.*

45. *Id.*

46. Hafez & Mullins, *supra* note 41, at 961.

47. *Id.*

48. Joseph Kunkle, *Social Media and the Homegrown Terrorist Threat*, POLICE CHIEF, June 2012, at 22.

49. Bates & Mooney, *supra* note 39, at 9.

50. Joel Alfredo Capellan & Alexei Anisin, *A Distinction Without a Difference? Examining the Causal Pathways Behind Ideologically Motivated Mass Public Shootings*, 22 HOMICIDE STUD. 235, 251 (2018).

51. *See id.* at 250.

52. Hafez & Mullins, *supra* note 41, at 961.

genders."[53] According to one study, in many cases, "group grievance interacts with mental disturbances . . . to drive individuals to ideologically motivated violence."[54] Social networks—facilitated by social media providers—can connect individuals who share similar grievances with radicals, creating a collective identity and promoting the diffusion of extreme ideologies.[55] Ideologies tend to "frame personal and collective grievances into broader political critiques of the status quo."[56] The collective may create an echo chamber, where members of the target group become the recepients of blame.[57] The collective demonizes these target groups and justifies violence against them.[58] Even in the absence of mental disturbance, group grievance still interacts with personal grievance to drive individuals to ideologically motivated violence.[59] This suggests that an interaction between group grievance and conditions that existed in an individual's life before involvement with the potential terrorist group causes most acts of terrorism.

With regard to international terrorism, online radicalization may occur in three stages.[60] During the first stage, individuals interested in learning more about a particular terrorist ideology will visit websites that describe the group's core beliefs.[61] During the second stage—indoctrination—these individuals accept the group's core beliefs and begin to look for ways to participate in advancing these beliefs.[62] Finally, the Internet allows these individuals to connect with other recruits "to plan and carry out their own attacks."[63]

It is clear then that the Internet and social media have become supporting structures and enabling environments for extreme ideologies to thrive.[64] The flexible, user-generated, and instantaneous nature of these applications helps extremist groups identify and communicate with potential recruits and build a sense of "communal belonging that is likely

53. Capellan & Anisin, *supra* note 50, at 244.

54. *Id.* at 251.

55. Hafez & Mullins, *supra* note 41, at 961, 964.

56. *Id.* at 961.

57. *See* Tate, *supra* note 10, at 1747. Most recently, in regard to the El Paso shooting, the group grievance was with Mexican immigration. *See* Gianluca Mezzofiore & Donie O'Sullivan, *El Paso Mass Shooting Is at Least the Third Atrocity Linked to 8chan This Year*, CNN (Aug. 5, 2019, 7:43 AM), https://www.cnn.com/2019/08/04/business/el-paso-shooting-8chan-biz/index.html [https://perma.cc/DA5C-ERBS].

58. Hafez & Mullins, *supra* note 41, at 961.

59. Capellan & Anisin, *supra* note 50, at 251.

60. *See* Anne Aly et al., *Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization*, 40 STUD. CONFLICT & TERRORISM 1, 4 (2017).

61. *Id.*

62. *Id.*

63. *Id.*

64. Hafez & Mullins, *supra* note 41, at 968.

to appeal to some alienated individuals."[65] These communities expand opportunities for radicalization by "validating extreme beliefs by likeminded radicals."[66] Even outside of the group context, social media facilitates the mass dissemination of propaganda.[67] There is empirical evidence that associates exposure to this propaganda, or other radical violent online material, with extremist attitudes and violence.[68] This relationship transcends the ideologies typically associated with international terrorism, with data suggesting that such exposure increases the risk that white supremacist and neo-Nazi groups will commit violent political acts.[69]

Thus, existing research addresses increased risk rather than definitive causation. Empirical evidence suggests that the Internet shapes decisions and, in combination with other offline factors, could be associated with decision-making in relation to violent acts.[70] Exposure to radical content is associated with an increased likelihood of political violence.[71] Individuals who seek violent radical material are also more likely than "passive seekers" to commit acts of political violence.[72] This suggests that a preexisting interest in violent extremism that was formed online acts as a motivator for these individuals to seek out additional information, which may in turn influence them towards violent extremism.[73] However, researchers note that it is unlikely that passive exposure to radical content will lead to political violence without an "underlying real-life motivation."[74]

On the other hand, the spread of radical information increases exposure to radical beliefs, which in turn may be the source of an individual's "underlying real-life motivation."[75] As mentioned above, groups seeking to radicalize individuals may target those with specific grievances and create an environment where that individual can assign blame for his grievances to a group.[76] Even if radicalization into political

65. *Id.* at 969; *see* Ghayda Hassan et al., *Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence*, 12 INT'L J. DEVELOPMENTAL SCI. 71, 72–73 (2018).

66. Hafez & Mullins, *supra* note 41, at 970.

67. *Id.*

68. Hassan et al., *supra* note 65, at 84.

69. *Id.* at 76, 83.

70. *Id.* at 84.

71. Schils & Pauwels, *supra* note 9.

72. Hassan et al., *supra* note 65, at 84.

73. Schils & Pauwels, *supra* note 9.

74. *Id.*

75. *See* DEP'T OF HOMELAND SEC., *supra* note 2, at 8 (describing how hostile actors use social media to "foment strife and division, and spur vulnerable individuals . . . to commit acts of violence").

76. *See* Capellan & Anisin, *supra* note 50, at 251; Hafez & Mullins, *supra* note 41, at 961.

violence requires a predisposition for those attitudes in an individual, social media is uniquely capable of amplifying and transmitting these beliefs to a large audience through social contagion.[77] Social contagion virtually guarantees that the message will reach individuals who are predisposed to violence and who may not have been accessible through other means.[78] Furthermore, recruitment tactics that domestic extremists and terrorist groups employ are similar to those international terrorist groups employ.[79]

III. HURDLES TO HOLDING SOCIAL MEDIA PROVIDERS LIABLE FOR ACTS OF TERRORISM

Successfully holding social media providers liable acts of terrorism (international or domestic) is nearly impossible because of protections offered to ISPs by the Communications Decency Act (CDA) and the courts' reluctance to find proximate cause in these cases.

A. *The Communications Decency Act (CDA)*

Although ISPs are popular targets for litigation, many lawsuits that may arise against them under the CDA are blocked. Social media providers have been subject to "lawsuits brought by victims of terror and their families for their alleged failure to curb the dissemination of material inciting terrorist activity."[80] Courts usually dismiss these cases quickly because of the blanket protection the CDA, codified at 47 U.S.C. § 230, grants to ISPs.[81] The CDA shelters ISPs from liability stemming from content posted by third-party users.[82] Specifically, the CDA bars civil claims against ISPs when "the content in question was posted by a third-party user," and the lawsuit "seeks to hold the defendant accountable as 'publisher or speaker' of that content."[83] The intent of the CDA is to "eliminate disincentives to self-regulation that had been

77. *See* Berger, *supra* note 43, at 62.

78. *Id.* (noting that social media "empowers . . . contact over wide geographical areas").

79. DEP'T OF HOMELAND SEC., *supra* note 2, at 10; *see* Emily Brown & William Munro, Ill. Wesleyan Univ., Address at the 28th Annual JWP Conference: Us vs. Them and Them vs. U.S.: A Comparative Analysis of Recruitment Strategies of the Islamic State and the Alt-right (Apr. 8, 2017).

80. Roter, *supra* note 16, at 1380–81.

81. 47 U.S.C. § 230(c)(1) (2018) (shielding social media providers from content they did not create); Roter, *supra* note 16, at 1381.

82. Roter, *supra* note 16, at 1381.

83. *Id.* at 1385 (quoting Lancaster v. Alphabet, Inc., No. 15-cv-05299-HSG, 2016 WL 3648608, at *2 (N.D. Cal. July 8, 2016)).

previously created by caselaw and . . . to actually *incentivize* self-regulation measures."[84]

Until recently, it was unclear whether the CDA shields social media providers from lawsuits plaintiffs bring under the ATA.[85] This led some commentators to suggest that the CDA may not immunize cases plaintiffs bring against ISPs under the ATA.[86] Under the material-support provisions of the ATA, plaintiffs may bring cases based on the consequences of an ISP allowing terrorist organizations to use the social media platform rather than on the specific content of the third party.[87]

If plaintiffs could use the ATA's material support provisions to circumvent the CDA, establishing the provision of material support could be a lower hurdle to overcome.[88] Recently, however, it appears that the strategy to circumvent the CDA with the ATA has not worked.[89] Courts have dismissed lawsuits almost immediately against social media providers within the terrorist context.[90] At least one court has reasoned that the ATA does not limit the CDA's protections of ISPs against civil liability and has been unwilling to consider acts that fall under the CDA immunity.[91]

B. *Proximate Cause Under the ATA*

Even if a lawsuit could make it past the CDA, courts have been reluctant to find proximate cause in cases plaintiffs bring against social media providers for acts of international terrorism.[92] Courts have seldom addressed causation because the CDA's blanket immunity prevents courts from hearing these cases.[93] When courts do address it, the proximate cause standard they apply varies.[94] Some courts apply a standard that plaintiffs satisfy when they show that harm resulting from the terrorist act was a foreseeable consequence of the defendant's

84. Goodman, *supra* note 28, at 179.

85. *See* Brown, *supra* note 37, at 4.

86. *See id.* at 11–12.

87. *See id.* at 4.

88. *See id.* at 17.

89. Freilich, *supra* note 16, at 678.

90. Roter, *supra* note 16, at 1394.

91. Force v. Facebook, Inc., 304 F. Supp. 3d 315, 324 (E.D.N.Y. 2018) (finding that the ATA does not limit civil liability protections under the CDA), *aff'd in part, dismissed in part*, 934 F.3d 53 (2d Cir. 2019), *cert. denied*, No. 19-859, 2020 WL 2515485 (U.S. May 18, 2020).

92. *See* Goodman, *supra* note 28, at 186.

93. *Id.* at 188 ("When the courts do not want to address proximate cause, they rest their denials on the CDA, but when they do not wish to address the CDA, they credit their dismissals to a lack of causation.").

94. *Id.* at 186.

actions.[95] More recent cases require a direct relationship between the plaintiff's injuries and the defendant's acts.[96]

Regardless of the standard courts use, the provision of material support in the form of providing a social media platform has not suggested a strong enough causal connection to the attack.[97] Current caselaw suggests that plaintiffs must allege and show that the terrorist organization used the social media platform as a "mechanism to carry out or plan deadly attacks."[98] Mere use of social media to spread extremist propaganda does not appear to be enough to demonstrate proximate cause of an attack.[99] Plaintiffs must be able to connect the website's content to the specific attacks.[100]

1. Fields v. Twitter, Inc.[101]

In *Fields*, a Jordanian police officer shot and killed two U.S. government contractors working at a law enforcement training center in Jordan.[102] ISIS claimed responsibility for the attack.[103] The plaintiffs sued Twitter under the ATA,[104] alleging that "Twitter provided material support to ISIS by allowing ISIS to sign up for and use Twitter accounts, and that this material support was a proximate cause of the . . . shooting."[105]

The plaintiffs alleged that ISIS used Twitter to spread propaganda, violent media, and tutorial content.[106] The plaintiffs also emphasized that ISIS used Twitter as a recruitment platform.[107] The trial court found that the plaintiffs did not adequately allege causation.[108] The court explained that the only connection between this specific act of terrorism and Twitter was that an execution that ISIS publicized on Twitter reportedly moved the gunman.[109] The court found this to be a weak causal connection, particularly because the plaintiffs based their argument on content disseminated through Twitter rather than the provision of Twitter

95. Brown, *supra* note 37, at 28.
96. *See* Goodman, *supra* note 28, at 186.
97. *See* Schwartz, *supra* note 17, at 1202.
98. *Id.*
99. *See id.*
100. *See id.*
101. 200 F. Supp. 3d 964 (N.D. Cal. 2016).
102. *Id.* at 966.
103. *Id.*
104. 18 U.S.C. § 2333(a) (2018).
105. *Fields*, 200 F. Supp. 3d at 966.
106. *Id.* at 967.
107. *Id.* at 967–68.
108. *Id.* at 973–74.
109. *Id.* at 974.

accounts.[110] The court further noted that the plaintiffs failed to explain how the provision of Twitter accounts to ISIS proximately caused the shootings.[111]

On appeal, the U.S. Court of Appeals for the Ninth Circuit articulated its standard for proximate cause under the ATA.[112] In doing so, the Ninth Circuit held that a plaintiff "must show at least some direct relationship between the injuries that he or she suffered and the defendant's acts" to satisfy the proximate cause requirement for civil liability under the ATA.[113] The court rejected the argument that the ATA standard for proximate cause requires only foreseeability.[114] Instead, the court found that the ATA standard for proximate cause presents a high hurdle for plaintiffs to overcome. The court reasoned that "[c]ommunication services and equipment are highly interconnected with modern economic and social life, such that the provision of these services and equipment to terrorists could be expected to cause ripples of harm to flow far beyond the defendant's misconduct."[115] The court also noted that nothing in the statute suggests that "Congress intended to provide a remedy to every person reached by these ripples" and that the language instead appeared to have a limiting purpose to prevent endless litigation.[116]

In *Fields*, the court noted that while "Twitter's alleged provision of material support to ISIS facilitated the organization's growth and ability to plan and execute terrorist acts," there was no connection between Twitter's provision of this aid and the plaintiff's injuries.[117] None of the facts the plaintiffs alleged indicated that the specific "attack was in any way impacted, helped by, or the result of ISIS's presence on the social network."[118] It seems then, following *Fields*, that plaintiffs who bring claims against social media providers need to provide evidence of a connection between the radical group's presence on social media and the specific attack, rather than a connection between its social media presence and increased political violence in general.[119]

110. *Id.*
111. *Id.*
112. Fields v. Twitter, Inc., 881 F.3d 739, 749 (9th Cir. 2018).
113. *Id.*
114. *Id.* at 748.
115. *Id.* at 749.
116. *Id.*
117. *Id.* at 749–50.
118. *Id.* at 750 (quoting Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1127 (N.D. Cal. 2016), *aff'd*, 881 F.3d 739 (9th Cir. 2018)).
119. *See id.*

2. Gonzalez v. Google, Inc.[120]

In *Gonzalez*, the plaintiffs alleged that the perpetrators of the Paris attacks "used . . . social media to build and maintain connections with ISIS recruits" and "used YouTube . . . for indoctrination and recruitment to ISIS."[121] The plaintiffs also alleged that the perpetrators posted a link to an ISIS recruiting video on YouTube in which they also appeared, and that other perpetrators "actively followed ISIS social media accounts and posted links to *jihadi* YouTube videos."[122] However, these connections were not strong enough to demonstrate "that Google's provision of the YouTube platform to ISIS 'had any direct relationship with the injuries' that Plaintiffs suffered."[123]

The plaintiffs further alleged that Google shared advertising revenue with ISIS, arguing that the "support contributed to the . . . attack because even if not used directly, [it] allowed other ISIS funds to be used to support the attack."[124] The court rejected this argument, reasoning that "the fact of fungibility does not modify the causal requirement imposed by the ATA's 'by reason of' element."[125] The plaintiffs did not meet the causal relationship because they failed to "allege [a] direct causal connection between the Paris attack and any shared revenue provided to ISIS" relating to the YouTube video that was generating the revenue.[126]

The court also dismissed the argument "that Google's . . . provision of material support to ISIS facilitated the organization's growth and ability to plan and execute terrorist attacks."[127] The court ultimately reasoned that none of these allegations were sufficient to meet the proximate cause requirement.[128]

3. Clayborn v. Twitter, Inc.[129]

In *Clayborn*, the plaintiffs attempted to hold Twitter, Google, and Facebook liable for a terrorist attack that killed fourteen people and injured twenty-two others in California.[130] The plaintiffs alleged "that by

120. 335 F. Supp. 3d 1156 (N.D. Cal. 2018), *appeal filed*, No. 18-16700 (9th Cir. Sept. 10, 2018).

121. *Id.* at 1178 (quoting Third Amended Complaint ¶¶ 332–39, *Gonzalez*, 335 F. Supp. 3d 1156 (No. 111), 2017 WL 6040930).

122. *Id.*

123. *Id.* (quoting *Fields*, 881 F.3d at 749).

124. *Id.* (alteration in original).

125. *Id.* at 1179 (quoting *Fields*, 881 F.3d at 749).

126. *Id.*

127. *Id.*

128. *Id.*

129. No. 17-cv-06894-LB, 2018 WL 6839754 (N.D. Cal. Dec. 31, 2018), *appeal filed*, No. 19-15043 (9th Cir. Jan. 8, 2019).

130. *Id.* at *1.

allowing 'foreign terrorist organizations' to use [Twitter, Google, and Facebook's] platforms, [the social media providers] aided and abetted international terrorism and provided material support to international terrorists."[131] The court declined to impose liability, explaining that "alleged radicalization through exposure to online content does not establish the necessary direct relationship between the defendants' conduct and the attacks on the victims."[132]

4. Crosby v. Twitter, Inc.[133]

Most recently, victims of the Pulse Night Club shooting brought suit against Twitter, Google, and Facebook under the ATA.[134] In *Crosby*, the plaintiffs argued that the shooter "viewed online content from ISIS and became 'self-radicalized.'"[135] The court found this connection tenuous and noted that the content did not compel the shooter's actions.[136] The plaintiffs also alleged that Twitter did not take a proactive enough approach to finding and removing ISIS accounts and that it failed to proactively monitor content, instead only reviewing content other users reported.[137] Further, the plaintiffs alleged that even when Twitter took these accounts down, it did nothing to prevent the creation of a new account immediately thereafter.[138] The plaintiffs' alleged connections between Twitter and the shooting were weak.[139] It was not enough that ISIS posted material online and that there was a generalized risk that someone sympathetic to its message could come across the posts.[140]

The court also hesitated because "if [it] accepted Plaintiffs' argument, Defendants would become liable for seemingly endless acts of modern violence simply because the individual viewed relevant social media

---

131. *Id.*

132. *Id.* at *8. The court continued,

> Moreover, the plaintiffs do not plead any facts that show any direct recruitment of the attackers by ISIS through the platforms or their radicalization by actual exposure to ISIS content on the defendants' sites. Absent concrete allegations such as these, other courts have held post-*Fields* that plaintiffs do not plausibly plead a direct ATA claim by alleging only that the social-media platforms radicalize users.

Id.

133. 921 F.3d 617 (6th Cir. 2019).

134. *Id.* at 619.

135. *Id.* at 625.

136. *Id.*

137. *Id.* at 620.

138. *Id.*

139. *Id.* at 621–22.

140. *Id.* at 622.

content before deciding to commit the violence."[141] The court suggested that social media providers "do not proximately cause everything that an individual may do after viewing this endless content."[142] Further, the court held that social media providers cannot "foresee how every viewer will react to third party content on their platforms," particularly in the case of independent criminal acts.[143] The court noted that the facts the plaintiffs alleged failed to connect the shooter to Twitter, and only generally connected the shooter to ISIS.[144] Indeed, the shooter became self-radicalized over a long period and only embraced ISIS directly prior to the attack; he was never directly in contact with ISIS.[145] This was insufficient to meet the ATA's proximate cause requirement.[146]

The court declined to consider whether providing routine social media services could be an act of international terrorism, leaving the question open.[147] Finally, the court acknowledged that there is a logical link between foreseeability and directness, and thus it is permissible for a court to assess foreseeability when determining proximate cause.[148]

IV. COULD LEGISLATIVE ACTION CREATE A CLEAR PATH TO HOLDING SOCIAL MEDIA PROVIDERS ACCOUNTABLE FOR DOMESTIC TERRORISM?

Recently, the discussion has increased on the merits of (1) modifying the ATA to include acts of domestic terrorism and (2) changing the CDA.

A. *Modifying the ATA to Include Acts of Domestic Terrorism*

Discussion has increased over whether courts should treat domestic terrorism the same as international terrorism, with some scholars arguing that the magnitude of the threat of domestic terrorism has increased.[149] Specifically, discussion has expanded over whether the ATA should include domestic terrorism.[150] Although some recourse is available to

141. *Id.* at 625.
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.* at 626.
147. *See id.* at 622.
148. *Id.* at 624.
149. *See* DEP'T OF HOMELAND SEC., *supra* note 2, at 8 (noting the recent increase in domestic terrorism). *But see* Francesca Laguardia, *Considering a Domestic Terrorism Statute and Its Alternatives*, 114 NW. U. L. REV. ONLINE 212, 215 (2019) ("[L]eveling the playing field between prosecutions of domestic and international terrorists would almost certainly encroach upon pure political speech.").
150. *See* Dilts, *supra* note 3, at 734. Some commentators suggest that Congress should amend the ATA to include domestic terrorism to force liability onto providers whose actions proximately cause harm. Tate, *supra* note 10, at 1769.

victims in tort, domestic terrorism is still terrorism and the federal government should treat it as such.[151] Including domestic terrorism under the ATA would signal that the federal government acknowledges the severity of the threat domestic terrorism poses and would elevate the moral wrongfulness of domestic terror attacks in the eye of the public.[152]

The line between domestic and international terrorism has always been blurred.[153] The government usually only classifies Islamic terror groups as "foreign terrorist organizations" but declines to apply the same designation to other terrorist ideologies with an international base.[154] The Internet has further muddied this distinction by enabling international terrorist groups to influence people from across the globe. [155] Attacks that may facially appear to be domestic terrorism may actually be internationally influenced.[156] One example of this is when foreign actors use social media to spread racist content to cause unrest domestically.[157] Treating domestic terrorism and international terrorism equally under the ATA would cover all acts of terrorism without requiring courts to painstakingly decide which kind of terrorism has occurred.

However, this change presents some difficulties in the context of social media. Currently, social media use only violates the ATA when a user is working with a foreign terrorist organization to share content that furthers the organization's goals.[158] Despite its underinclusiveness, the ATA typically applies to specifically designated terrorist groups, which

151. *See* Dilts, *supra* note 3, at 724; Tate, *supra* note 10, at 1761.

152. McQuade, *supra* note 14; *see* DEP'T OF HOMELAND SEC., *supra* note 2, at 23 (identifying the importance of increasing societal awareness of violent extremism and mobilization to violence).

153. *See* McQuade, *supra* note 14.

154. Sinnar, *supra* note 2, at 1347–48 (describing the government's classification of white supremacists as domestic terrorists, despite the ideology's global network and reach).

155. Tony Romm, *Facebook CEO Mark Zuckerberg Says in Interview He Fears 'Erosion of Truth' but Defends Allowing Politicians to Lie in Ads*, WASH. POST (Oct. 17, 2019, 3:32 PM), https://www.washingtonpost.com/technology/2019/10/17/facebook-ceo-mark-zuckerberg-says-interview-he-fears-erosion-truth-defends-allowing-politicians-lie-ads/ [https://perma.cc/D84V-BQ8L].

156. *See id.* (discussing how Mark Zuckerberg blamed the United States' weak response to Russia's interference for the fact that other countries, including China and Iran, are catching on to disinformation campaigns).

157. Julian E. Barnes & Adam Goldman, *Russia Trying to Stoke U.S. Racial Tensions Before Election, Officials Say*, N.Y. TIMES (Mar. 10, 2020), https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html [https://perma.cc/YZP8-EVD2] (describing Russia's efforts to use social media "to incite violence by white supremacist groups and to stoke anger among African-Americans"); *see* DEP'T OF HOMELAND SEC., *supra* note 2, at 11 (acknowledging that domestic terrorists "often find the online space crucial as they grow closer to mobilizing to violence" and that "[t]hese threats may be exacerbated by foreign actors seeking to undermine the Homeland through disinformation campaigns").

158. VanLandingham, *supra* note 29, at 48.

makes it easier to determine when an ISP materially supports terrorism.[159] On the other hand, members of groups with extreme ideologies that may not classify as terrorist organizations perpetrate many acts of domestic terrorism.[160] Domestic terrorists are often lone wolves and may be advancing a goal of the group without directly planning the attack with it.[161] Unless the federal government expands its list to include specific domestic terrorist groups, it may be difficult for ISPs to determine which users and posts to remove.

Even if Congress does not modify the ATA to treat domestic and international terrorism equally, there are still signs that Congress is paying more attention to domestic terrorism. Recently, Congress introduced the "Domestic Terrorism Prevention Act of 2019."[162] The bill identifies "[w]hite supremacists and other far-right-wing extremists" as "the most significant domestic terrorism threat facing the United States" and aims to "require the federal government to take steps to prevent domestic terrorism."[163] Three Texas Congressmen introduced the Domestic Terrorism Penalties Act of 2019 in the House around the same time which seeks to amend the ATA to directly penalize acts of domestic terrorism.[164] Although the bill lists offenses and penalties, there is no indication that the current material support or civil liability provisions will extend to include acts of domestic terrorism.[165]

B. *Modifying the CDA*

Many commentators suggest that Congress should amend the CDA to preclude use of its shield in ATA cases.[166] Some argue that the CDA was never meant to protect ISPs that provide material support to terrorists.[167] Since courts continue to protect ISPs, some scholars suggest that

159. *See* Trevor Aaronson, *Terrorism's Double Standard*, INTERCEPT (Mar. 23, 2019, 8:34 AM), https://theintercept.com/2019/03/23/domestic-terrorism-fbi-prosecutions/ [https://perma.cc/M2AG-LXW7].

160. *Id.*

161. *See* ALLISON G. SMITH, U.S. DEP'T OF JUSTICE, HOW RADICALIZATION TO TERRORISM OCCURS IN THE UNITED STATES 8 (2018); BJELOPERA, *supra* note 9, at 2, 53 (noting that "terrorist lone actors (lone wolves) . . . generally operate autonomously and in secret, all the while drawing ideological sustenance—*not direction*—from propagandists operating in the free market of ideas" and that "lone wolves potentially adopt the ideas of broader terrorist movements while not claiming formal membership in them").

162. S. 894, 116th Cong. § 1 (2019).

163. *Id.* §§ 1–2.

164. H.R. 4187, 116th Cong. § 2 (2019).

165. *See* McQuade, *supra* note 14.

166. *See* Freilich, *supra* note 16, at 678–79; Roter, *supra* note 16, at 1382.

167. Nicole Phe, Note, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99, 127 (2018).

Congress should clarify that the CDA is not meant to shield ISPs from liability stemming from providing material support to terrorists.[168] The scholars point to § 230(e)(1) of the CDA, which states that "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute."[169] If domestic terrorism were included under the ATA, material support to domestic terrorists would become a federal crime. With this clarification, the CDA would not act as a barrier to plaintiffs bringing a civil action under the ATA, especially if a criminal trial under the ATA came first.[170]

Although Congress initially enacted the CDA to encourage ISPs to self-moderate, in reality, it has encouraged complacency.[171] Some commentators suggest that ISPs should be forced to comply with takedown requests but should not be expected to monitor content on their own.[172] Other commentators argue that courts should require ISPs to actively monitor and screen for terrorist content.[173] Still, others argue that courts should limit the shield to ISPs that make good faith efforts to restrict abusive material.[174]

A better approach would be to limit the CDA's blanket immunity to claims that specifically relate to the publication of user-generated content.[175] This would remove automatic protections for ISPs that plaintiffs accuse of materially supporting terrorists because liability "does not depend on the manner in which aid was provided."[176] However, if the aid ISPs provide does involve user-generated content, the CDA's immunity should still apply to ISPs that make a good faith attempt to

168. *See, e.g.*, Alexander Tsesis, *Social Media Accountability for Terrorist Propaganda*, 86 FORDHAM L. REV. 605, 624 (2017).

169. 47 U.S.C. § 230(e)(1) (2018); *see* Tsesis, *supra* note 168, at 623–24.

170. Tsesis, *supra* note 168, at 624.

171. Freilich, *supra* note 16, at 691 ("Because social media companies cannot be sued for damages for content provided by another user, there is no economic incentive to innovate to solve the issue of terrorist propaganda being widely distributed through ISPs. . . . [E]ven though nonprofit companies are ready and willing to develop systems to identify and block terrorist content, social media companies are not eager to take advantage of such systems."); Phe, *supra* note 167, at 125 ("[O]verzealously extending this broad immunity to ISPs neither incentivizes nor motivates them to implement measures . . . .").

172. Caitlin McKeown, Comment, *Facebook, Defamation, and Terrorism: Who Is Responsible for Dangerous Posts on Social Media?*, 26 TUL. J. INT'L & COMP. L. 163, 181 (2017); Roter, *supra* note 16, at 1382.

173. *See, e.g.*, Phe, *supra* note 167, at 128.

174. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 416–17 (2017).

175. *Id.* at 415.

176. *Id.* at 415–16.

mitigate this aid.[177] Limiting the good faith requirement only to causes of action that do not specifically relate to the publication of user-generated content but factually involve user-generated content would preserve more CDA protections outside of the criminal context and thus allow ISPs to focus their resources on moderating content that presents more of a danger to human life.

Removing blanket immunity in this narrow context would incentivize ISPs to take a more active role in making sure terrorists do not use their platforms and would give the courts more discretion to decide the cases on the merits.[178] Removing immunity, rather than imposing sweeping requirements and regulation, would also allow ISPs to determine their method of detection and prevention.[179] The courts would then have discretion to determine whether the ISPs' efforts were reasonable under the circumstances.[180]

Without legislative modifications, plaintiffs can continue bringing suit against social media providers, in the hope of eventually eroding the CDA's grant of immunity. Some scholars argue that the scope for immunity under the CDA is already narrowing,[181] with caselaw suggesting that a suit could succeed under a failure to warn theory.[182] Recently, courts also seem more willing to hold ISPs accountable for third-party content when the ISPs are notified of the content and do not take it down.[183]

C. *Proximate Cause for Acts of Domestic Terrorism*

The existing caselaw seems to condemn holding social media providers liable for acts of terrorism, particularly in light of the existing evidence that focuses on the radicalization process.[184] On the other hand, the court in *Crosby* did not preclude liability completely, noting that one should not interpret its holding to mean that "[d]efendants could never proximately cause a terrorist attack through their social media

177. *Cf. id.* at 416 (arguing that courts should apply this good faith requirement to every defendant before allowing CDA protections).

178. *Id.* at 416, 418.

179. *Id.* at 418–19.

180. *Id.* at 419. In determining reasonableness, courts could consider the nature of the "aid" the ISP provided and whether it took appropriate measures to prevent the act of terrorism given the ISP's characteristics. *Id.* Some relevant characteristics may include the ISP's size, financial resources, and the nature of the services it provides. One would expect a greater terrorist threat from ISPs that have a greater proportion of user-generated content.

181. *See* Tsesis, *supra* note 168, at 623.

182. McKeown, *supra* note 172, at 171.

183. Roter, *supra* note 16, at 1397.

184. *See* discussion *supra* Section III.B.

platforms."[185]Although plaintiffs have been largely unsuccessful in proving causation for acts of international terrorism, perhaps causation would be easier to demonstrate in instances of domestic terrorism.

The targets of domestic terrorism are often more specific and predictable.[186] While international terrorist organizations appear to influence attacks that indiscriminately target American citizens, homegrown domestic terrorism fixates on particular target groups, often based on race or sex.[187] Online discussions about domestic-target groups may make it easier to predict where acts of domestic terrorism will occur and whom the attacks will target.[188] Domestic terror groups are also more likely to consist of Americans, who often respond to events more locally.[189] Since many perpetrators of mass attacks often make "threatening or concerning communications" leading up to the attacks, these attacks may be easier to identify and prevent because they are more likely to name identifiable domestic locations.[190]

Although social media providers may argue that it is unduly burdensome for them to identify and delete posts that incite violence, there are alternative methods, including only holding these providers accountable for content users report.[191] Furthermore, technologies are

185. Crosby v. Twitter, Inc., 921 F.3d 617, 625 (6th Cir. 2019).

186. BJELOPERA, *supra* note 9, at 6 (discussing how domestic terrorists seek to further a specific cause or ideology).

187. *See id.*; DEP'T OF HOMELAND SEC., *supra* note 2, at 10 ("Domestic terrorist attacks and hate crimes sometimes overlap, as perpetrators of prominent domestic terrorist attacks have selected their targets based on factors such as race, ethnicity, national origin, religion, sexual orientation, gender, and gender identity.").

188. *See Signs of Possible Terrorist Activity*, METROPOLITAN POLICE, https://www.met.police.uk/advice/advice-and-information/t/terrorism-in-the-uk/signs-of-possible-terrorist-activity/ [https://perma.cc/ER5X-T3QE] (identifying "messages intended to stir up hatred against any religious or ethnic group" and "speeches or essays calling for racial or religious violence" as "signs of possible online terrorist activity"). *But see* DEP'T OF HOMELAND SEC., *supra* note 2, at 24 (noting that "[n]umerous studies have confirmed that peers with the closest proximity to individuals at risk of radicalization to violent extremism are uniquely positioned to detect, prevent, and counter this process" and advocating for a localized prevention approach).

189. *See* BJELOPERA, *supra* note 9, at 3, 15.

190. DEP'T OF HOMELAND SEC., *supra* note 2, at 22 (discussing themes evident among perpetrators of targeted violence).

191. McKeown, *supra* note 172, at 181. Recently, Facebook has revamped its counterterrorism team. *See* Davey Alba et al., *Facebook Expands Definition of Terrorist Organizations to Limit Extremism*, N.Y. TIMES (Sept. 18, 2019), https://www.nytimes.com/2019/09/17/technology/facebook-hate-speech-extremism.html# [https://perma.cc/PP5S-6VNU]; David Uberti, *Facebook Went to War Against White Supremacist Terror After Christchurch. Will It Work?*, VICE (Oct. 3, 2019, 11:20 AM), https://www.vice.com/en_us/article/vb5yk3/facebook-went-to-war-against-white-supremacist-terror-after-christchurch-will-it-work [https://perma.cc/G248-LH5P] (explaining how Facebook expanded its definition of terrorism to cover more

constantly improving, with some suggesting that social media providers may identify speech that may lead to an attack.[192]

Importantly, courts have dismissed many cases because the plaintiff failed to draw a connection between the social media provider and the actual instance of terrorism.[193] If this connection were made, what would it look like? Foreign terrorist organizations frequently use social media to radicalize users.[194] In cases of domestic terrorism, however, radicalization would look different.[195] ISIS inundates Twitter with propaganda, but one can identify this content easily.[196] In cases of domestic terrorism, the line is increasingly blurry: content that some would consider mere political expression others may interpret as a radical incitement of violence.[197] With growing political polarization, it may be even harder for ISPs to identify posts domestic terrorists create for recruitment or radicalization, even if they wanted to.[198]

However, none of the above cases dealt with an affirmative action on the part of the social media provider. Recently, Congress questioned Mark Zuckerburg, the CEO of Facebook, about the website's advertising policy.[199] Zuckerberg's answers suggest that Facebook bans direct calls for violence and racist content, but it does not have a procedure in place that actively monitors the content of political advertisements.[200] Furthermore, these political advertisements can target users based on demographic criteria.[201] Thus, it is possible that Facebook or other ISPs

---

domestic threats but will still allow politicians to use hate speech that does not overtly incite violence).

192. *See* Katie Cohen et al., *Detecting Linguistic Markers for Radical Violence in Social Media*, 26 TERRORISM & POL. VIOLENCE 246, 253 (2014).

193. *See* discussion *supra* Section III.B.

194. Hafez & Mullins, *supra* note 41, at 969.

195. BJELOPERA, *supra* note 9, at 48.

196. *See* Berger, *supra* note 43, at 63.

197. Uberti, *supra* note 191; *see* BJELOPERA, *supra* note 9, at 49 ("A 2016 study found that Americans espousing white supremacist ideals on the social-media platform Twitter outnumber the supporters of the foreign terrorist organization known as the Islamic State by many measures . . . .").

198. *See* Uberti, *supra* note 191.

199. This questioning was in the context of politicians creating advertisements that spread false information, but one could easily use these ads to spread politicized false information about specific groups. *See* Romm, *supra* note 155; *see also* Mike Isaac, *Dissent Erupts at Facebook over Hands-Off Stance on Political Ads*, N.Y. TIMES (Oct. 28, 2019), https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-political-ads.html [https://perma.cc/VV8H-RNDZ] (reporting that many Facebook employees are also concerned about misinformation).

200. *See* Uberti, *supra* note 191.

201. Raphael Cohen-Almagor, *The Role of Internet Intermediaries in Tackling Terrorism Online*, 86 FORDHAM L. REV. 425, 435 (2017).

do take a more active role in recruitment to a particular ideology.[202] This may take the form of a group targeting Facebook users that are most likely to radicalize with advertisements designed to inflame a group grievance.[203] In this way, the website is no longer simply hosting content, but it is actively promoting specific content to specific users.[204] In an era where Internet use is more personal, a court may find it foreseeable that terrorist recruiters would take advantage of these tools to narrow their audience.[205] Although the ATA's test requires a direct connection between the social media platform and the attack, at least some courts view foreseeability as an essential component of the proximate cause analysis and acknowledge that "directness and foreseeability are logically linked."[206]

Yet this still may not be enough to demonstrate a direct connection to the act of terrorism, unless the act was a part of the advertisements. In the case of domestic terrorism, "lone wolf" members of dissatisfied groups carry out many acts of political violence.[207] If the members of these groups publicly encourage the "lone wolf" to carry out the attack, this would be different from the recruitment or radicalization arguments that courts have been reluctant to accept.[208] Instead of simply providing a platform for radicalization, the social media provider would be providing a platform for extremists to gather, plan, and encourage attacks.[209]

---

202. *See* Freilich, *supra* note 16, at 697–98 (discussing how ISPs may profit from advertisements that target those viewing extremist content).

203. *See* Hafez & Mullins, *supra* note 41, at 961 (presenting the factors that produce extremism).

204. One can also use this technology for counterterrorism purposes. *See* DEP'T OF HOMELAND SEC., *supra* note 2, at 24 ("DHS will engage the technology sector to identify and amplify credible voices online, and promote counternarratives against violent extremist messaging."); Freilich, *supra* note 16, at 698 (discussing available technology that can target antiterrorist advertising towards ISIS sympathizers to educate them).

205. Use of these tools by terrorist organizations may be particularly foreseeable when the repeated abuse of them has been well documented and linked to at least one attack. *See* Sam Dean, *Facebook Decided Which Users Are Interested in Nazis—And Let Advertisers Target Them Directly*, L.A. TIMES (Feb. 21, 2019, 5:00 AM), https://www.latimes.com/business/technology/la-fi-tn-facebook-nazi-metal-ads-20190221-story.html [https://perma.cc/PAD6-WKAV].

206. Crosby v. Twitter, Inc., 921 F.3d 617, 624 (6th Cir. 2019) (quoting Kemper v. Deutsche Bank AG, 911 F.3d 383, 392 (7th Cir. 2018)).

207. BJELOPERA, *supra* note 9, at 53.

208. This would be different because a specific person is the target, which has a closer nexus to the eventual attack than broad, undirected recruitment or radicalization efforts. *See* Clayborn v. Twitter, Inc., No. 17-cv-06894-LB, 2018 WL 6839754, at *8 (N.D. Cal. Dec. 31, 2018) (noting that absent concrete allegations that ISIS directly recruited the attackers through Twitter, or the attackers' actual exposure to ISIS content on Twitter, there is no plausible ATA claim), *appeal filed*, No. 19-15043 (9th Cir. Jan. 8, 2019).

209. 8chan is one example of an ISP providing this kind of support. *See After Reports the El Paso Shooter Posted a Manifesto, 8chan Went Dark. But Is It Gone for Good?*, ABC NEWS (Aug.

Empirical data suggest that these groups are effective and that membership in these groups leads to increased political violence.[210] Perhaps if the plaintiff can demonstrate that the social media provider knew domestic terrorists were using its platform to plan a specific act of domestic terrorism and the provider failed to intervene, the connection would be direct enough to hold the provider liable under the ATA.[211]

CONCLUSION

Although change is on the horizon, it is unclear whether these changes will be enough to provide victims of domestic terrorism with the recourse they seek. Amending the ATA and CDA will grant courts more opportunity to address proximate cause for acts of domestic terrorism facilitated by social media, and courts are likely to continue to rely on stringent tests to analyze causation. Even if the proximate cause analysis effectively blocks most victims of domestic terrorism from obtaining relief, amending the ATA and CDA to allow for holding social media providers liable in cases of domestic terrorism will still have benefits in terms of prevention.

Legislation that includes domestic terrorism in the ATA or otherwise recognizes domestic terrorism as an equal threat will have enormous benefits. Treating domestic and international terrorism equally under the law would signal the federal government's interest in taking an active role in prevention.[212] This would allow the allocation of resources generally reserved for combating foreign terrorism.[213] This would also allow for the federal prosecution of individuals planning a domestic attack.[214]

Legislation that rolls back the CDA's blanket immunity would also be beneficial. It is undisputed that social media has played a key role in the expansion of domestic terrorism.[215] Holding social media providers liable where the plaintiff can prove proximate cause will encourage larger providers to take reasonable steps to prevent acts of domestic terrorism.[216]

5, 2019), https://www.abc.net.au/news/2019-08-06/8chan-is-down2c-but-is-it-gone-for-good/11386304 [https://perma.cc/U3LC-27KH].

210. Hassan et al., *supra* note 65, at 84.

211. *See* McKeown, *supra* note 172, at 184.

212. *See* Dilts, *supra* note 3, at 726.

213. McQuade, *supra* note 14 (arguing that elevating domestic terrorism would enable "long-term, proactive investigations that can detect and disrupt terror plots before they occur").

214. *Id.*

215. *See* BJELOPERA, *supra* note 9, at 48.

216. Freilich, *supra* note 16, at 691.