10-1-2016

Fight Terror, Not Twitter: Insulating Social Media From Material Support Claims

Nina I. Brown

FIGHT TERROR, NOT TWITTER: INSULATING SOCIAL MEDIA FROM MATERIAL SUPPORT CLAIMS

NINA I. BROWN*

Social media companies face a new threat: as millions of users around the globe use their platforms to exchange ideas and information, so do terrorists. Terrorist groups, such as ISIS, have capitalized on the ability to spread propaganda, recruit new members, and raise funds through social media at little to no cost. Does it follow that when these terrorists attack, social media is on the hook for civil liability to victims?

Recent lawsuits by families of victims killed in terrorist attacks abroad have argued that the proliferation of terrorists on social media—and social media's reluctance to stop it—violates the Antiterrorism Act. This article explores the dangers associated with holding social media companies responsible for such attacks and offers a solution to avoid liability.

This is a new challenge for social media and there is little to no scholarship on the topic. This article examines the basis for this liability—the Antiterrorism Act—as it relates to suits against social media and section 230 of the Communications Decency Act, which provides that an interactive computer service (broadly defined to include a variety of websites, including social media platforms) cannot be treated as the publisher or speaker of third-party content.

This article argues that section 230 of the Communications Decency Act should provide immunity for social media outlets from suits based on the actions of its users. This is in spite of the fact that courts have traditionally interpreted section 230 to immunize content providers for liability from the *content* posted by third parties, as opposed to the acts of those parties themselves.

---

*Assistant Professor, S.I. Newhouse School of Public Communications, Syracuse University, 215 University Place, Syracuse, NY 13244.

I. INTRODUCTION

Carl Fields, a military contractor stationed in Amman, Jordan, was shot and killed while eating lunch in the staff cafeteria of the police-training center where he worked.[1] Although the gunman appeared to be acting alone, ISIS claimed responsibility for the attack. Carl's widow blames Twitter.

She argues that the fault lies with Twitter because it knowingly permitted "ISIS to use its social network as a tool for spreading extremist propaganda, raising funds and attracting new recruits."[2] This usage has been instrumental in ISIS's ability to carry out numerous terrorist attacks including the one that took her husband's life.[3]

Reynaldo Gonzalez agrees. His daughter Nohemi was shot and killed during a terrorist attack in Paris while dining with friends at a local bistro.[4] Nohemi was a student at California State University, Long Beach studying in Paris for the semester.[5] Five other terrorist attacks took place in Paris that same night and ISIS claimed responsibility for all of them.[6] Like Ms. Fields, Mr. Gonzalez has sued social media—Twitter, Facebook, and YouTube (Google)—arguing that its laissez-faire approach to terrorists on its sites caused the death of his daughter.[7]

Plaintiffs in both cases claim the legal basis for liability lies in United States antiterrorism laws, which prohibit providing material support to

---

1. Complaint at ¶ 71, Fields v. Twitter, Inc., No. 4:16-CV-00213-KAW (N.D. Cal. filed Jan. 13, 2016); Taylor Luck & William Booth, *Gunman in Jordan Kills 5, Including 2 Americans, at Police Training Site*, WASH. POST (Nov. 9, 2015), http://www.washingtonpost.com/world/middle_east/report-2-americans-killed-in-jordan-shooting-at-security-training-site/2015/11/09/63cdf6f8-86da-11e5-be8b-1ae2e4f50f76_story.html [http://perma.cc/SKY7-SQGV].

2. Complaint, *supra* note 1, at ¶ 1.

3. *Id.*

4. Verified Complaint at ¶ 111, Gonzalez v. Twitter, Inc., No. 3:16-cv-03282 (N.D. Cal. filed June 14, 2016).

5. *Id.* at ¶ 110.

6. *Id.* at ¶¶ 112–13.

7. *Id.* at ¶¶ 120–21.

known terrorists and offer civil relief to families of victims.[8] Specifically, plaintiffs argue that by knowingly allowing ISIS to use their social networks as tools for spreading extremist propaganda, raising funds, and attracting new recruits, the defendants violated the Antiterrorism Act ("ATA").[9]

Ms. Fields's lawsuit was the first attempt to hold a social media company civilly liable under the ATA.[10] Mr. Gonzalez filed suit five months later under the same theory of liability.[11] These cases likely represent the first in a wave of cases against social media platforms brought by bereaved families. It is too early to know whether these claims against social media will ultimately be successful, but these suits ring an alarm in the social media industry.

Social media platforms often claim immunity from suits for civil liability from harm flowing from content on their platforms under section 230 of the Communications Decency Act ("CDA").[12] This provision protects Internet providers from liability for content—posts, pages, comments, tweets, etcetera—created by its users.[13]

These cases represent a new challenge for courts. The suit brought by Ms. Fields was the first attempt to allege liability against social media platforms under the antiterrorism laws. And though significant literature

---

8. *See, e.g.*, 18 U.S.C. § 2331 (2001).

9. Though it probably will not be the last, particularly if Ms. Fields's suit is successful in any measure. And why not? There is no point in suing ISIS, Hamas, or other terrorist network and there has been an increase in litigation against enterprises that provide material support to those organizations. *See* Suzanne Northington, *Congressional Bill Asks Companies to Disclose Boards' Cybersecurity Expertise*, WESTLAW J. COMPUTER & INTERNET, Jan. 2016, at 1 (noting that lawyers who specialize in terrorism say that Fields is likely facing an uphill battle).

10. Marnie O'Neill, *Tamara Fields Sues Twitter Over Murder of Husband Lloyd 'Carl' Fields by IS Operative*, NEWS.COM.AU (Jan. 15, 2016, 4:53 PM), http://www.news.com.au/technology/online/social/tamara-fields-sues-twitter-over-murder-of-husband-lloyd-carl-fields-by-is-operative/news-story/872169f17161be10a20b4a30de365218 (last visited Oct. 22, 2016).

11. *See generally* Verified Complaint, *supra* note 4.

12. 47 U.S.C. § 230 (2013) (providing immunity for online publishers for content posted by third parties); *see infra* Section IV.

13. *Id.* § 230.

has analyzed the broad reach of material support provisions,[14] there is an exceptionally limited amount of scholarship regarding liability for social media companies.[15]

Of note, there is currently no scholarship exploring whether section 230[16] might insulate social media companies from liability in cases brought under the ATA.[17] The application of section 230 is unclear where liability is based not on the content posted by the third-party, but instead on the consequences of allowing that third party to use the social media platform. This is a critical distinction and presents a second unsettled question for courts confronting these cases.

This article explores both issues. Section I examines the likelihood that the ATA could result in liability for Twitter and other social media companies that provide platforms on which ISIS organizes, raises money, and recruits. Though the discussion is not limited to the set of facts at issue in *Fields v. Twitter* and *Gonzalez v. Twitter*, these cases are used as a framework for analyzing such claims. Section II evaluates the strength of legal arguments social media platforms could make in defense of these claims. However, even assuming social media could obtain defense verdicts based on the facts, it does nothing to stop the flow of suits—plaintiffs will continue to make claims against social media giants

---

14. *See generally* Noah Bialostozky, *Material Support of Peace? The On-the-Ground Consequences of U.S. and International Material Support of Terrorism Laws and the Need for Greater Legal Precision*, 36 YALE J. INT'L. L. ONLINE 59 (2011); Nina J. Crimm, *High Alert: The Government's War on the Financing of Terrorism and its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 WM. & MARY L. REV. 1341 (2004); James J. Ward, Note, *The Root of All Evil: Expanding Criminal Liability for Providing Material Support to Terror*, 84 NOTRE DAME L. REV. 471 (2008). *See also* David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1, 10 (2003).

15. Only two law journals have published articles somewhat related to this issue. *See* Emily Goldberg Knox, Note, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295, 308 (2014) (discussing terrorist use of social media and material support implications, but not considering section 230 of the Communications Decency Act as a solution); Paulina Wu, Comment, *Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.*, 16 CHI. J. INT'L L. 281, 283 (2015) (discussing the increased use of social media by terrorists and arguing that the United Nations has an important role to play in regulating such content, but not examining the material support concerns or possible section 230 resolution).

16. 47 U.S.C. § 230 (providing immunity for online publishers for content posted by third parties); *see infra* Section IV.

17. This conclusion is based on extensive searches resulting in no scholarship.

believing in either a strong set of facts that justifies a judgment or hoping for a sympathetic judge. Thus, the litigation costs remain high—each company will have to litigate each respective case on the facts. A better solution for social media to have a more favorable outcome would be to win on the law—if section 230 applies, case dismissed. Section III reviews the applicability of section 230 of the CDA to the ATA and section IV concludes that even though the application of section 230 is imprecise, it should shield social media from liability.

II. BACKGROUND

A. *The Attacks*

Both Carl Fields, Jr. and Nohemi Gonzalez were shot and killed in apparent terrorist attacks in November 2015. Nohemi, a student at California State University, Long Beach studying in Paris for the semester, was killed in the Paris attacks while dining with friends at a local bistro.[18] Carl was killed while working at the United States-funded Jordan International Police Training Centre ("JIPTC").[19]

The JIPTC is a facility that trains Palestinian and Iraqi police officers.[20] On November 9, 2015, Anwar Abu Zaid, an officer studying at the training center, smuggled an assault rifle with 120 bullets and two handguns into the center.[21] Abu Zaid first shot a truck moving through the facility, killing an American.[22] He then entered the cafeteria and killed four additional people who were eating lunch, including Carl.[23]

Though the Jordanian government explained the attack as a "lone wolf" attack inspired by ISIS, ISIS itself claimed responsibility for the

18. Verified Complaint at ¶¶ 110–11, Gonzalez v. Twitter, Inc., No. 3:16-cv-03282 (N.D. Cal. filed June 14, 2016).

19. *See* Complaint at ¶¶ 67, 71, Fields v. Twitter, Inc., No. 4:16-CV-00213-KAW (N.D. Cal. filed Jan. 13, 2016).

20. *See id.* at ¶ 67.

21. *See id.* at ¶¶ 69–71.

22. *See id.* at ¶ 71.

23. *See id.*

attack and issued a warning:[24] "Do not provoke the Muslims more than this, especially recruited and supporters of the Islamic State."[25] ISIS continued: "The more your aggression against the Muslims, the more our determination and revenge . . . time will turn thousands of supporters of the caliphate on Twitter and others to wolves."[26] ISIS supporters commended the shooting on Twitter,[27] which took place on the ten-year anniversary of ISIS's coordinated bomb attacks on three hotels in Amman, Jordan on November 9, 2005.[28] The statement further included a chronological list of attack claims that included the November 13th Paris massacre.[29]

B. *Social Media and Terror*

ISIS's mention of Twitter in its statement is not surprising. There is little question that ISIS, in addition to several other Designated Foreign

---

24. Bridget Johnson, *ISIS Claims Lone Wolf Attack in Jordan that Killed Two Americans*, PJ MEDIA (Nov. 16, 2015), http://pjmedia.com/blog/isis-claims-lone-wolf-attack-in-jordan-that-killed-two-americans/ [http://perma.cc/Z6DX-AWHE] (The Jordanian government took the position that the attack had no link to terrorist groups. The shooter, Abu Zaid, was killed by security forces.); Jonathan Stempel & Alison Frankel, *Twitter Sued by U.S. Widow for Giving Voice to Islamic State*, REUTERS (Jan. 14, 2016, 5:15 PM), http://www.reuters.com/article/us-twitter-isis-lawsuit-idUSKCN0US1TA20160114 [http://perma.cc/AQ86-DNXA]; *see also* Complaint, *supra* note 19, at ¶ 71 (According to the complaint, ISIS reiterated its responsibility for the attacks in its Dabiq Magazine, Issue 12: "And on '9 November 2015,' Anwar Abu Zeid—after repenting from his former occupation—attacked the American crusaders and their apostate allies, killing two American crusaders, two Jordanian apostates, and one South African crusader. These are the deeds of those upon the methodology of the revived Khilāfah. They will not let its enemies enjoy rest until enemy blood is spilled in revenge for the religion and the Ummah.").

25. Johnson, *supra* note 24 (also claiming the Russian Metrojet over the Sinai on Halloween and the Burj el-Barajneh bombings in the Beirut suburbs on November 12).

26. *Id.*

27. *See* Complaint, *supra* note 19, at ¶ 75 ("With one user tweeting: 'The killing shall continue and will not stop.'").

28. Taylor Luck & William Booth, *Gunman in Jordan Kills 5, Including 2 Americans, at Police Training Site*, WASH. POST (Nov. 9, 2015), http://www.washingtonpost.com/world/middle_east/report-2-americans-killed-in-jordan-shooting-at-security-training-site/2015/11/09/63cdf6f8-86da-11e5-be8b-1ae2e4f50f76_story.html [http://perma.cc/SKY7-SQGV].

29. Johnson, *supra* note 24.

Terrorist Organizations ("DFTOs"), routinely uses Twitter and other social media to organize, recruit, fundraise, and inspire violence.[30] For example, there are active Twitter accounts for the Popular Front for the Liberation of Palestine and Kata'ib Hezbollah, among others.[31] Terrorists are online: they are on Facebook, Twitter, YouTube, and other social media platforms to network, data mine, and share information.[32] Their online presence is staggering: "[A]bout 90 percent of organized terrorism on the internet is being carried out through social media."[33] The reason is simple: social media tools are inexpensive, accessible, and allow groups to disseminate unfiltered information to a broad audience in real time.[34]

The increased presence of terrorist organizations on social media has generated a growing concern that groups like ISIS are increasingly using these communication sites in sophisticated ways.[35] The fear is that terrorist organizations use these sites "to spread their propaganda and training, allowing the disaffected worldwide to be radicalized in the privacy of their

---

30. *See* Alan F. Williams, *Prosecuting Website Development Under the Material Support to Terrorism Statutes: Time to Fix What's Broken*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 365, 396 (2008) ("Terrorism experts have reached a consensus that the Internet is a particularly 'effective and important tool of contemporary terrorists.'"); *see also* Michael Holmes, *ISIS Looking For Recruits Online*, WWLP (June 20, 2014, 11:00 PM), http://wwlp.com/2014/06/20/isis-looking-for-recruits-online/ [http://perma.cc/2E4Y-25PB] (noting that "supporters of the Jihadist group have also launched a public relations offensive online; blitzing sites like Facebook, Twitter and Youtube with their extremist message."). *See generally* Gabriel Weimann, *New Terrorism and New Media*, WILSON CENTER: COMMONS LAB 1 (2014), http://www.wilsoncenter.org/publication/new-terrorism-and-new-media [http://perma.cc/B6MW-SEPJ].

31. *See* Zoe Bedell & Benjamin Wittes, *Tweeting Terrorists, Part I: Don't Look Now But a Lot of Terrorist Groups are Using Twitter*, LAWFARE (Feb. 14, 2016, 5:05 PM), http://www.lawfareblog.com/tweeting-terrorists-part-i-dont-look-now-lot-terrorist-groups-are-using-twitter [http://perma.cc/G2UK-7BWN].

32. *See* Williams, *supra* note 30, at 396.

33. *Terrorist Groups Recruiting Through Social Media*, CBC NEWS (Jan. 10, 2012, 2:24 PM), http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social-media-1.1131053 (last visited Sept. 28, 2016).

34. *See* Paulina Wu, Comment, *Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.*, 16 CHI. J. INT'L L. 281, 283 (2015).

35. Elizabeth Weise, *Facebook, Twitter Pressured to do More to Halt Terrorists*, USA TODAY (Dec. 11, 2015, 6:03 PM), http://www.usatoday.com/story/tech/2015/12/07/facebook-twitter-social-media-terrorism-lawmakers-feinstein/76948528/ [http://perma.cc/ZF7L-DFYB].

homes."[36] Terrorism expert Rita Katz observed that "[f]or several years, ISIS followers have been hijacking Twitter to freely promote their jihad with very little to no interference at all . . . . Twitter's lack of action has resulted in a strong, and massive pro-ISIS presence on their social media platform, consisting of campaigns to mobilize, recruit and terrorize."[37] According to a report published by J.M. Berger and Heather Perez in February 2016 regarding the presence of ISIS on Twitter, there are approximately 3,000 ISIS-supporting Twitter accounts active at any given time.[38]

Terrorists have used Facebook to identify sympathizers and disseminate bomb-making instructions.[39] Further, terrorists have used Facebook "as a gateway to extremist sites and other online radical content; it acts as a media outlet for terrorist propaganda and extremist ideological messaging and provides a mechanism to share operational and tactical information."[40] They use YouTube to share propaganda videos, communicate, and recruit.[41] More recently, "terrorists have used Instagram and Flickr to glorify Osama Bin Laden, for example, or document the execution of hostages."[42]

The United States government is paying attention to the influx of terrorist activity on social media sites. The Obama Administration recently held a summit in Silicon Valley to collaborate with technology companies

---

36. *Id.*

37. Alex Altman, *Why Terrorists Love Twitter*, TIME (Sept. 11, 2014), http://time.com/3319278/isis-isil-twitter/ [http://perma.cc/S9R2-4E4T].

38. J.M. Berger & Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters*, GW PROGRAM ON EXTREMISM 1, 4 (Feb. 2016), http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf [http://perma.cc/B7Q2-UNVW] (noting that Twitter and Facebook are the two main platforms used by ISIS supporters to spread their propaganda).

39. Emily Goldberg Knox, Note, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295, 299–300 (2014).

40. Wu, *supra* note 34, at 289.

41. Knox, *supra* note 39, at 300.

42. Wu, *supra* note 34, at 289.

on ways to combat terrorism.[43] However, the government is not necessarily waiting for technology companies to cooperate: legislators have introduced legislation that would require technology companies to report online terrorist activity to law enforcement.[44] The recent dispute between Apple and the FBI regarding the iPhone belonging to one of the San Bernardino shooters provides a clear example of "how far the government is willing to push tech companies in the name of fighting terrorism."[45]

C. *The Response to Date*

The response of social media companies to terrorists' use of their services is varied[46] but has been trending towards proactivity in removing content posted by terror groups.[47] Of course, some companies are more committed to this than others but there may be a new reason for all social media to take a more active position in the fight against terror.

Initially, social media companies were slow to react to terrorists' use of their sites.[48] This began to change when social media became the outlet

---

43. Jenna McLaughlin, *White House Raises Encryption Threat in Silicon Valley Summit*, INTERCEPT (Jan. 8, 2016, 11:35 AM), http://theintercept.com/2016/01/08/white-house-raises-encryption-threat-in-silicon-valley-summit/ [http://perma.cc/84XY-EW4M].

44. *See, e.g.*, Press Release, Diane Feinstein, U.S. Senator for Cal., Bill Would Require Tech Companies to Report Online Terrorist Activity (Dec. 8, 2015) (on file on Diane Feinstein's official website) [http://perma.cc/88SZ-5QEJ] ("We're in a new age where terrorist groups like ISIL are using social media to reinvent how they recruit and plot attacks."). After heavy lobbying by social media, the bill was withdrawn. It was recently reintroduced by Senator Feinstein. *See Could Twitter Stop the Next Terrorist Attack?*, CBS NEWS (July 24, 2015, 10:49 AM), http://www.cbsnews.com/news/could-twitter-stop-the-next-terrorist-attack/ [http://perma.cc/T9M9-LX9M].

45. Kaveh Waddell, *The Government Is Secretly Huddling with Companies to Fight Extremism Online*, ATLANTIC (Mar. 9, 2016), http://www.theatlantic.com/technology/archive/2016/03/the-government-is-secretly-huddling-with-companies-to-fight-extremism-online/472848/ [http://perma.cc/TN2Q-VRXW].

46. Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015, 7:00 AM), http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ [http://perma.cc/6ZV5-QDBL].

47. *Id.*

48. Helle Dale, *Why ISIS Has Threatened the CEOs of Facebook and Twitter*, DAILY SIGNAL (Feb. 27, 2016), http://dailysignal.com/2016/02/27/why-isis-has-threatened-the-ceos-of-facebook-and-twitter/ [http://perma.cc/8PS4-6Z7Q]; Greenberg, *supra* note 46.

to spread videos and images of journalist James Foley's beheading.[49] Facebook, for example, began actively policing against terrorists' use of its service: "The world's largest social network is [now] quicker to remove users who back terror groups and investigates posts by their friends. It has assembled a team focused on terrorist content and is helping promote 'counter speech,' or posts that aim to discredit militant groups like [the] Islamic State."[50] These policing efforts have made a difference: Facebook has been more successful than other sites at blocking ISIS-related accounts and content.[51] Still, social media platforms are reluctant to be seen as a tool of the government.

Twitter has taken a different approach from Facebook and does not monitor or actively police content. Though the company has recently "condemn[ed] the use of [its services] to promote terrorism,"[52] Twitter has "maintained one of the most liberal free speech policies among major social networks,"[53] thereby positioning itself as a defender of free speech.[54] In a January 2011 blog post entitled "The Tweets Must Flow," Twitter co-

---

49. Greenberg, *supra* note 46.

50. Natalie Andrews & Deepa Seetharaman, *Facebook Steps Up Efforts Against Terrorism*, WALL ST. J. (Feb. 11, 2016, 7:39 PM), http://www.wsj.com/articles/facebook-steps-up-efforts-against-terrorism-1455237595 (last visited Sept. 28, 2016).

51. Brian Mastroianni, *Could Policing Social Media Help Prevent Terrorist Attacks?*, CBS NEWS (Dec. 15, 2015, 7:15 AM), http://www.cbsnews.com/news/could-policing-social-media-prevent-terrorist-attacks/ [http://perma.cc/N8DB-5YYY].

52. Twitter, *Combating Violent Extremism*, TWITTER BLOG (Feb. 5, 2016, 8:13 PM), http://blog.twitter.com/2016/combating-violent-extremism [http://[perma..cc/LS83-AQNP].

53. Jessi Hempel, *Twitter's Latest Challenge: Deciding Who's a Terrorist*, WIRED (Jan. 8, 2016, 7:00 AM), http://www.wired.com/2016/01/twitters-latest-challenge-is-deciding-whos-a-terrorist/ [http://perma.cc/HFX9-JRPZ].

54. *See, e.g.*, Holmes, *supra* note 30 (noting that Twitter founder Biz Stone—who is no longer with the company— responded to media questions about ISIS's use of Twitter to publicize its acts of terrorism by saying: "[i]f you want to create a platform that allows for the freedom of expression for hundreds of millions of people around the world, you really have to take the good with the bad."); Deana Kjuka, *When Terrorists Take to Social Media*, THE ATLANTIC (Feb. 20, 2013), http://www.theatlantic.com/international/archive/2013/02/when-terrorists-take-to-social-media/273321 [http://perma.cc/9TZN-N835]; Somini Sengupta, *Twitter's Free Speech Defender*, N.Y. TIMES (Sept. 2, 2012), http://www.nytimes.com/2012/09/03/technology/twitter-chief-lawyer-alexander-macgillivray-defender-free-speech.html.

founder Biz Stone and Twitter General Counsel Alex MacGillivray wrote: "We don't always agree with the things people choose to tweet, but we keep the information flowing irrespective of any view we may have about the content."[55] In its *defender* role, Twitter denied every removal request (126 in total) made by the United States Government in 2015.[56] Twitter has thus demonstrated a concern for protecting speech even in the face of a countervailing government interest.

The tension between Twitter's hands-off approach to content regulation and terrorist organizations' embrace of social media came to a head this year when Tamara Fields and Reynaldo Gonzalez sued social media for the deaths of their loved ones. In both cases, plaintiffs claimed that social media knowingly permitted ISIS to use their social networks as tools for spreading extremist propaganda, raising funds and attracting new recruits in violation of the ATA.[57] The ATA prohibits providing *material support* to terrorist organizations and offers a civil claim for relief to victims.[58]

Although it is too early to know whether these claims against social media will ultimately be successful,[59] these suits should raise the hackles of

---

55. Biz Stone, *The Tweets Must Flow*, TWITTER BLOG (Jan. 28, 2011, 8:13 PM), http://blog.twitter.com/2011/the-tweets-must-flow [http://perma.cc/7254-6NSQ] (While this post was written in the wake of the Egyptian Revolution in January 2011 and was not aimed at ISIS's presence on the platform, Twitter has largely remained steadfast in its dedication to free-flowing speech on the website).

56. *Removal Requests-January to June 2015*, TWITTER TRANSPARENCY REPORT, http://transparency.twitter.com/removal-requests/2015/jan-jun [http://perma.cc/6N7Q-8CQ6]; *Removal Requests-July to December 2015*, TWITTER TRANSPARENCY REPORT, http://transparency.twitter.com/en/removal-requests.html#removal-requests-jul-dec-2015 [http://perma.cc/2GGR-ZP3H]. This includes requests made by a government agency, police, and other authorized reporters.

57. Though it probably will not be the last, particularly if Ms. Fields's suit is successful in any measure. And why not? There is no point in suing ISIS, Hamas, or any other terrorist network and there has been an increase in litigation against enterprises that provide material support to those organizations. *See* Suzanne Northington, *Congressional Bill Asks Companies to Disclose Boards' Cybersecurity Expertise*, WESTLAW J. COMPUTER & INTERNET, Jan. 2016, at 14 (noting that lawyers who specialize in terrorism say that Fields is likely facing an uphill battle).

58. 18 U.S.C. § 2331 (2001).

59. Though based on the facts of these cases, to be discussed in Sections I–III, *infra*, I suspect this is doubtful.

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

Importantly, the United States government has expressed a preference for enhanced security over speech when it comes to terrorism.[60] Preventing terrorism is a priority and the government has already prosecuted several founders and administrators of websites with known links to terrorism under the ATA and has been vocal about the need to deprive terrorists of these tools.[61] In addition, the government has emphasized the need to frustrate DFTOs' efforts to exploit social media to further their terrorist agenda, specifically calling on Twitter— often without success—to shut down particular accounts linked to known terrorists.[62] The ATA offers victims of terrorism a civilly-based means of redress for the exact same grievances—providing support to terrorists—regardless of whether the government has prosecuted the conduct or not. A closer look at the statute

60. *See* McLaughlin, *supra* note 43.

61. Knox, *supra* note 39, at 308; Williams, *supra* note 30, at 400 ("The Internet is a critical tool for modern terrorist organizations, and the U.S. government, like those of other countries, has a substantial interest in regulating advocacy on this medium that is specifically intended to encourage violent attacks on the United States and its citizens—particularly messages targeted to assist in the recruitment of a new crop of terrorists and efforts designed to raise funds for terrorist organizations."); *see also* Hillary Clinton, *My Plan to Defeat ISIS*, MEDIUM (Dec. 7, 2015), http://medium.com/hillary-for-america/my-plan-to-defeat-isis-769a7f485ace#.a3y2fr8ax [http://perma.cc/FT3F-KZBA]; Liz Kreutz, *Hillary Clinton Calls on Facebook, YouTube, and Twitter to Help With Fight Against ISIS*, ABC NEWS (Dec. 6, 2015, 11:47 AM), http://abcnews.go.com/Politics/hillary-clinton-calls-facebook-youtube-twitter-fight-isis/story?id=35607324 (last visited Sept. 28, 2016).

62. Michael Isikoff, *Twitter Under Pressure to Act More Aggressively Against Terrorists*, YAHOO! NEWS (Feb. 18, 2015), http://news.yahoo.com/twitter-under-pressure-to-act-more-aggressively-against-terrorists-230347109.html [http://perma.cc/9MH2-TCFG].

and recent case law suggests that an unfavorable outcome for social media is certainly plausible.[63]

III. COULD THE MATERIAL SUPPORT LAWS RESULT IN LIABILITY FOR SOCIAL MEDIA?

Social media makes it possible for people around the world to disseminate information to wide audiences and stay connected with others at a low cost. Its utility reaches traditional news media organizations, celebrities, athletes, corporations, private citizens, and everyone in between, including terrorists. Of course, ISIS and other terrorist organizations use social media not because the platforms were made for or offered exclusively to them, but rather because the services are available to *everyone*.

Twitter, for example, boasts hundreds of millions of users.[64] Worldwide, users post over 500 million tweets per day.[65] That is 6,000 tweets per second. Given this volume, it may seem far-fetched that without endorsing or promoting a terrorist organization's tweets, Twitter could face liability.

But the ATA does not premise liability merely on whether it is Twitter's *purpose* to further the goals of the terrorist organization. Instead, the statute only requires a showing that Twitter had knowledge or exhibited deliberate indifference in providing material support to a terrorist

---

63. Professor David Cole has described that the material support statute is written so broadly that it penalizes anything a defendant has done that benefits a group that has been identified by the government as a DFTO. David Cole, Address to the Terrorism & Justice Conference: Less Safe, Less Free: A Progress Report on the War on Terror (Feb. 18, 2008), *in* J. INST. JUST. & INT'L STUD., 1, 6 ("This law basically allows the government to get a so-called "terrorism conviction" without proving that the defendant, engaged in any terrorist act, conspired to engage in any terrorist act, aided or abetted any terrorist act, or ever intended to further any kind of terrorism."); *see also* David Cole, *Is Hamas's Twitter Account Illegal?*, DAILY BEAST (Nov. 20, 2012, 9:30 AM), http://www.thedailybeast.com/articles/2012/11/20/is-hamas-s-twitter-account-illegal.html [http://perma.cc/JJ7Z-BNER] ("[T]he 'material support' law is written so broadly that it makes virtually anything one does to or for a designated group a crime, even if it has no link to terrorist activity of any kind.").

64. Complaint at ¶ 60, Fields v. Twitter, Inc., No. 4:16-CV-00213-KAW (N.D. Cal. filed Jan. 13, 2016).

65. *Twitter Usage Statistics*, INTERNET LIVE STATS, http://www.Internetlivestats.com/twitter-statistics/#trend [http://perma.cc/PJS7-DDPF].

organization.[66] As Professor Cole explains, "[t]he material support law is a classic instance of guilt by association. It imposes liability regardless of an individual's own intentions or purposes, based solely on the individual's connection to others who have committed illegal acts."[67] It should come as no surprise then that this is exactly what the complaints in the current cases allege: that Twitter and other social media were insufficiently attentive to the abuse of their platforms by terrorist organizations such as ISIS.[68]

Accordingly, the operative legal question is not whether social media offers a service directly or exclusively to terrorist organizations, but rather whether those companies are aggressive enough in their response to addressing the use of their services by people and organizations they know to be terrorists. In short, the defendants could face liability if they knowingly provided a platform on which terrorists could recruit, raise funds, and/or mobilize.

This broad exposure to liability is precisely what Congress intended: the legislation aimed to reach those that made it possible for terrorist organizations to carry out attacks.[69] Thus, the material support provision covers a significant amount of otherwise harmless conduct.[70] The legislative history indicates that "the crux of the ATA was to provide plaintiffs with certainty that a valid right of action against terrorist acts would be available to vindicate their injuries."[71] The material support provisions thus specifically target those who have assisted terrorist

---

66. 18 U.S.C. § 2339 (2012); Weiss v. Nat'l Westminster Bank PLC, 768 F.3d 202, 208 (2d Cir. 2014).

67. David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1, 10 (2003).

68. *See* Verified Complaint at ¶¶ 110–11, Gonzalez v. Twitter, Inc., No. 3:16-cv-03282 (N.D. Cal. filed June 14, 2016); Complaint, *supra* note 64, at ¶¶ 69–71.

69. H.R. REP. NO. 102-1040, at 5 (1992); Peter Budoff, Note, *How Far Is Too Far? The Proper Framework for Civil Remedies Against Facilitators of Terrorism*, 80 BROOK. L. REV. 1057, 1082 (2015).

70. *See* Cole, *supra* note 67, at 13 (noting that "the material support law presumes that even a donation of crayons to a day-care center affiliated with Hamas will 'facilitate' terrorism").

71. H.R. REP. NO. 102-1040, at 5; Jesse D. H. Snyder, Note, *Reading Between the Lines: Statutory Silence and Congressional Intent Under the Antiterrorism Act*, 1 BRIT. J. AM. LEGAL STUD. 265, 269 (2012).

organizations in certain specific ways.[72] "The concern is . . . that if people are allowed to speak, associate, and support [terrorist] organizations freely, those organizations might be strengthened, and might take dangerous action in the future."[73]

Thus, Congress recognized that the ATA needed to be broad to further the policy goals of assigning liability to financial supporters of terrorism.[74] Despite this clear intent, courts have struggled to reconcile the ATA with traditional tort law principles that warn against imposing strict liability on those without strong and obvious connections to terrorism.[75] The result of this struggle is that it is uncertain whether claims under the ATA against social media companies are viable.

A. *Civil liability Under the ATA*

When initially enacted in 1986, the ATA was meant to provide an avenue for victims of international terrorism to bring claims in United States courts against those who perpetrated the attack.[76] Under the current civil remedies provision, liability expands beyond terrorist organizations, many of which are jurisdictionally out of reach.[77] The current version

---

72. Snyder, *supra* note 71, at 271.

73. David Cole, *Out of the Shadows: Preventive Detention, Suspected Terrorists, and War*, 97 CALIF. L. REV. 693, 724 (2009) (noting that the problem "is that while some people tried and convicted for "material support" may pose a real threat to the nation's security, the laws' overbreadth means that many who do not pose such a threat may nonetheless fall within their proscriptions. In this sense, they are inaccurate proxies for actual dangerousness, and, as preventive measures, are vastly overinclusive.").

74. *Id.*

75. Abecassis v. Wyatt, 704 F. Supp. 2d 623, 664 (S.D. Tex. 2010).

76. *See* Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 494 (E.D.N.Y. 2012) (explaining that the legislation was in many ways a response to two terrorist attacks—the attack by the PLO of the Achille Lauro cruiseliner and the bombing of Pan Am flight 103 over Lockerbie, Scotland by Libyan terrorists).

77. 18 U.S.C. § 2333(a) (1994); H.R. REP. NO. 102-1040, at 5; Geoffrey Sant, *So Banks Are Terrorists Now?: The Misuse of the Civil Suit Provision of the Anti-Terrorism Act*, 45 ARIZ. ST. L.J. 533, 534 (2013) (noting that this change was made because few terrorists maintain assets in the United States and as such, "not a single reported decision so much as referenced the ATA's civil suit provision during its first decade in existence").

offers victims[78] of international terrorism a remedy to sue for civil damages against not only the terrorist organizations but also those who provide them with *material support*.[79] Under the present statute, United States nationals who have been injured as a result of illegal[80] and violent acts abroad may pursue these claims in United States courts.[81]

Claims against social media companies based on violations of material support under the ATA are likely to be predicated on violations of sections 2339A and 2339B, both of which prohibit providing material support to terrorists and terrorist organizations.[82] Thus, a claimant would argue that he or she is entitled to civil damages based on the social media company's provision of services to terrorists, which is a violation of section 2339A and 2339B.

Indeed, both Ms. Fields and Mr. Gonzalez have predicated their entitlement to a civil remedy under section 2333 on violations of sections 2339A and 2339B of the ATA.[83] The arguments are that the defendant social media companies knew or reasonably should have known that ISIS used their services.[84] And because ISIS used those services to spread extremist propaganda, raise money, and attract recruits; the defendants' provision of that platform satisfied the definition of material support.[85]

Despite the fact that the statute itself is silent on what a plaintiff needs

---

78. 18 U.S.C. § 2333(a) (Under the statute, the survivor may sue as well has his or her estate, survivors, or heirs).

79. Weiss v. Nat'l Westminster Bank PLC, 768 F.3d 202, 206–07 (2d Cir. 2014); *Gill*, 893 F. Supp. 2d at 492.

80. Under section 2331, international terrorism is defined to include "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State." 18 U.S.C. § 2331 (2012).

81. *Id.*

82. 18 U.S.C. § 2339 (2012).

83. Complaint, *supra* note 64, at ¶¶ 79–86 (alleging that Twitter purposefully, knowingly, or with willful blindness provided to ISIS support and services which constitute *material support* to a Foreign Terrorist Organization).

84. Complaint, *supra* note 64, at ¶ 80; Verified Complaint, *supra* note 68, at ¶ 9.

85. Complaint, *supra* note 64, at ¶ 1.

to prove to succeed on a claim under section 2333,[86] courts have generally required three factors: (1) an unlawful action—here, the provision of material support; (2) the requisite mental state; and (3) causation.[87]

1. What counts as *material support*?

Establishing the provision of material support is the lowest hurdle when it comes to claims against social media and other web-service providers. It is immaterial that the platforms (e.g., Twitter, Facebook, YouTube) are not themselves illegal.[88] Material support is broadly defined[89]—it includes both communications equipment and other tangible and intangible property and services:

> [T]he term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments, or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.[90]

---

86. Wultz v. Islamic Republic of Iran, 755 F. Supp. 2d 1, 55 (D.D.C. 2010) (explaining that Congress did not explicitly set out the elements that a private plaintiff would be required to plead and prove to recover. Instead, it "intended to *incorporate general principles of tort law* . . . into the [civil] cause of action under the ATA.") (emphasis added); *see also* S. REP. NO. 102-342, at 45 (1992) ("This section creates the right of action, allowing any U.S. national who has been injured in his person, property, or business by an act of international terrorism to bring an appropriate action in a U.S. district court. *The substance of such an action is not defined by the statute, because the fact patterns giving rise to such suits will be as varied and numerous as those found in the law of torts*. This bill opens the courthouse door to victims of international terrorism.") (emphasis added).

87. Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 502 (E.D.N.Y. 2012).

88. *See* David Cole, *Is Hamas's Twitter Account Illegal?*, DAILY BEAST (Nov. 20, 2012, 9:30 AM), http://www.thedailybeast.com/articles/2012/11/20/is-hamas-s-twitter-account-illegal.html [http://perma.cc/JJ7Z-BNER].

89. *See id.*

90. 18 U.S.C. § 2339A(b)(1) (2012).

A service that offers individuals and organizations the ability to network and communicate fits neatly into the above definition. Twitter offers a service that allows users to send and read short 140 character messages called *tweets*, join back-channels, and link to outside content.[91] Facebook offers an interactive service that allows users to create profiles; post commentary, links, images, and videos; and interact with other users both via private messages and public posts on other users' "walls."[92] YouTube offers a service that allows users to upload and comment on videos.[93]

Consequently, the material support element should be easy for any plaintiff seeking to use the material support provisions in this way, such as Ms. Fields and Mr. Gonzalez.

In fact, the government has already prosecuted founders and administrators of websites with known links to terrorism under the material support statute.[94] The Department of Justice has gone further "suggest[ing] that website administrators would be held criminally liable for terrorist activity on their websites."[95] Thus, there is little question that the services provided by social media constitute material support as defined in the statute.

2. The *knowledge* requirement.

The Supreme Court has construed the definition of material support

---

91. *See generally* TWITTER, www.twitter.com [http://perma.cc/2BTK-ND62].

92. *See generally* FACEBOOK, http://www.facebook.com [http://perma.cc/BMY8-ZAUX].

93. *See generally* YOUTUBE, http://www.YouTube.com [http://perma.cc/2SS7-XWUH].

94. Emily Goldberg Knox, Note, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 295, 308–09 (2014) (giving examples, including that "in 2010, the DOJ charged Zachary Chesser, the founder of a radical website, with attempting to provide material support to a designated FTO"); Mattathias Schwartz, *How Dangerous Were the Edmonds Cousins?*, THE NEW YORKER (Mar. 31, 2015), http://www.newyorker.com/news/news-desk/how-dangerous-were-the-edmonds-cousins [http://perma.cc/C57V-ZPHP]; David Smith, *81% of ISIS-Linked Suspects Charged in US are American Citizens*, GUARDIAN (Nov. 20, 2015, 9:07 AM), http://www.theguardian.com/world/2015/nov/20/isis-suspects-us-citizens-syria [http://perma.cc/TCW3-JG2H].

95. Knox, *supra* note 94, at 308.

broadly.[96] In so doing, the Court made clear that the critical question in any given case will be whether knowingly allowing terrorists to use the service can be viewed as material support.[97] Here, the relevant inquiry is how much knowledge social media companies would need to have about terrorists' activities on their platforms to satisfy the mens rea requirement.

Section 2333 of the ATA, which offers the civil remedy to victims, does not include a mens rea requirement on its face.[98] Instead, courts have incorporated one from the relevant statutory provisions—here, section 2339A and section 2339B(a)(1).[99] Section 2339A criminalizes the provision of material support to terrorists *if the defendant knew* that the support would be used in preparation for, or in carrying out, violations of certain criminal laws, or if the defendant *intended* the support to be so used.[100] This section presents an immediate—and likely insurmountable—hurdle for many plaintiffs challenging social media, including Ms. Fields and probably Mr. Gonzalez, as it requires a higher degree of knowledge or intent that the support or resources are used in executing violent federal crimes.[101]

---

96. Holder v. Humanitarian Law Project, 561 U.S. 1, 16–17 (2010).

97. *See* Boim v. Holy Land Found. for Relief & Dev. (*Boim II*), 549 F.3d 685, 690 (7th Cir. 2008) (en banc majority opinion) (The case discussed the parents of a United States national who was fatally shot in Israel by terrorists and sued several parties, including a charity that provided humanitarian support to Hamas. The Seventh Circuit held that even though giving money is not a violent act, "[g]iving money to Hamas, like giving a loaded gun to a child (which also is not a violent act), is an 'act dangerous to human life.'").

98. *See* 18 U.S.C. § 2333 ("(a) Action and jurisdiction. –Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees; (b) Estoppel under United States law. –A final judgment or decree rendered in favor of the United States in any criminal proceeding under section 1116, 1201, 1203, or 2332 of this title or section 46314, 46502, 46505, or 46506 of title 49 shall estop the defendant from denying the essential allegations of the criminal offense in any subsequent civil proceeding under this section; (c) Estoppel under foreign law. –A final judgment or decree rendered in favor of any foreign state in any criminal proceeding shall, to the extent that such judgment or decree may be accorded full faith and credit under the law of the United States, estop the defendant from denying the essential allegations of the criminal offense in any subsequent civil proceeding under this section.").

99. *See* Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 504 (E.D.N.Y. 2012).

100. 18 U.S.C. § 2339A (2012).

101. *Id.*; Knox, *supra* note 94, at 308 (noting that "[w]ithout direct evidence, it would be

Section 2339B is broader and requires only knowledge that material support or resources are being provided, not that they are being used for terrorism.[102] Accordingly, section 2339B offers plaintiffs asserting claims against social media the best chance for recovery.[103] It requires only that the defendant knowingly provided, attempted to provide, or conspired to provide material support or resources to a foreign terrorist organization.[104] Thus, defendants do not need to know that their support is furthering terrorism or illegal activities: "knowledge about the organization's connection to terrorism" is enough.[105] Courts have held that an organization's "knowing provision of material support" to a terrorist organization (or its deliberate indifference as to whether or not it provided material support to a terrorist organization) qualifies as sufficient knowledge to hold it accountable.[106] Simply put, this is not a high standard.

For example, in a case against Twitter based on an attack carried out by ISIS, for Twitter to demonstrate it lacked knowledge, it would have to show that it legitimately did not know, and could not find out, whether ISIS ran various accounts. On the other hand, Twitter would have acted with

---

far-fetched to assert that legitimate businesses, such as social media companies, act intending to promote federal terrorism crimes").

102. 18 U.S.C. § 2339B (2012).

103. *Id.* (As noted above, the statute requires knowledge or intent that the material support is being used for terrorism and therefore is a less viable option as applied here.).

104. *Gill*, 893 F. Supp. 2d at 504.

105. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 16–17 (2010) (holding that "Congress plainly spoke to the necessary mental state for a violation § 2339B, and it chose knowledge about the organization's connection to terrorism, not specific intent to further the organization's terrorist activities"); *see also* Knox, *supra* note 94, at 308 ("As mentioned above, § 2339A is not a viable option as applied to the activities of social media companies because of the specific intent requirement. Section 2339B, however, which requires only 'knowledge about the organization's connection to terrorism,' could conceivably be applied to social media websites used by designated FTOs who claim on their account profile to be acting on behalf of such an organization.").

106. *Boim II*, 549 F.3d at 698 ("To give money to an organization that commits terrorist acts is not intentional misconduct unless one either knows that the organization engages in such acts or is deliberately indifferent to whether it does or not, meaning that one knows there is a substantial probability that the organization engages in terrorism but one does not care."); Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287, 331 (E.D.N.Y. 2015).

the requisite mental state if it knew that ISIS operated certain accounts to further the terrorist group's goals and did nothing to stop the accounts.[107] To avoid a finding of knowledge under the statute, Twitter would have to remove all accounts it knew to be affiliated with ISIS. Twitter could not avoid knowledge by arguing that it offers a communications platform ubiquitously available to anyone and that the platform was not specifically aimed at terrorists.

This reading of the mens rea requirement would not be problematic for Twitter if it could simply argue that it does not know who runs a particular account. However, Twitter cannot be deliberately indifferent as to whether ISIS operates certain accounts.[108]

This, of course, is where things get complicated. Twitter, along with Facebook and Google, knows that ISIS and other terrorist organizations use their platforms. United States government officials have identified these sites as crucial communication tools used by ISIS.[109] Commentators and activists have acknowledged the problem.[110] Indeed, Twitter itself has acknowledged it: in a public statement posted after the Fields' suit was filed, Twitter claims to have suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily those related to ISIS.[111] Notably, online anti-terror activists, including the group *Anonymous*, have disputed Twitter's assertions, claiming that *Anonymous* is actually responsible for the majority of the account suspensions.[112]

---

107. *Linde*, 97 F. Supp. 3d at 331.

108. *Boim II*, 549 F.3d at 693; *Gill*, 893 F. Supp. 2d at 506.

109. *See* discussion *supra* Section II, pp. 9–10.

110. *See, e.g.*, Alan F. Williams, *Prosecuting Website Development Under the Material Support to Terrorism Statutes: Time to Fix What's Broken*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 365, 396 (2008); Paulina Wu, Comment, *Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N.*, 16 CHI. J. INT'L L. 281, 283 (2015).

111. Twitter, *Combating Violent Extremism*, TWITTER BLOG (Feb. 5, 2016, 8:13 PM), http://blog.twitter.com/2016/combating-violent-extremism [http://perma.cc/LS83-AQNP].

112. Joshua Philipp, *Hackers Say Twitter Isn't Telling the Whole Story About Anti-Terror Fight*, EPOCH TIMES (Mar. 4, 2016, 10:54 PM), http://www.theepochtimes.com/n3/1983519-hackers-say-twitter-isnt-telling-the-whole-story-about-anti-terror-fight/ [http://perma.cc/5826-XQ6A]; Complaint, *supra* note 64, at ¶ 61 (This is because Twitter does not independently search for problematic accounts but instead relies on user reports. These activists further claim that Twitter has actually been suspending accounts of the users reporting online terrorism as well: "Members of the community have taken this as a slap in the face. While Twitter is telling the

Putting aside for the moment who is responsible for the account suspensions, it must be noted that these takedowns reduce the "amount of pro-ISIS content available on Twitter . . . ." As accounts are shut down, followers are lost and "individual users who repeatedly created new accounts after being suspended [suffer] devastating reductions in their follower counts."[113] ISIS then responds with countermeasures, such as using applications and "simple hacking techniques to quickly create new accounts for users who have been suspended, as well as elaborate tactics to rebuild follower networks."[114] As this game of whack-a-mole plays out, "more than 20,000 Twitter accounts supporting ISIS across multiple languages" are still live.[115] And the operative question becomes: are Twitter, Facebook, YouTube, or any other social media company sitting at the defendants' table doing *enough*?

At its core, any ATA claim against social media is premised on a claim that the site knowingly let ISIS exploit its services because it was not attentive enough to the problem; in short, it was *deliberately indifferent*. In her case, Ms. Fields alleges that Twitter knew of the rampant use of its platform by ISIS (such use was widely reported by news organizations, for example) and that it did not do enough to stop it.[116] This argument is bolstered by the fact that Twitter does not actively police its site for content violations.[117] Instead, Twitter relies on users reporting violations.[118]

---

public it's working to stop ISIS recruitment on its services, it has been suspending accounts of the community that is doing the actual footwork."); P.W. Singer & Emerson Brooking, *Terror on Twitter*, POPULAR SCIENCE (Dec. 11, 2015), http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media [http://perma.cc/7YGH-FHRG] (Where it is explained that while Twitter has provided a passive stance and will remove accounts that are reported as terrorists, hacktivist groups such as Anonymous have launched active attacks and "hunting" initiatives to find and take down terror accounts on Twitter.).

113. J.M. Berger & Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters*, GW PROGRAM ON EXTREMISM 1, 4 (Feb. 2016), http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf [http://perma.cc/B7Q2-UNVW].

114. Berger & Perez, *supra* note 113, at 4.

115. Ians, *The Reach of ISIS Dwindling on Twitter*, TECHRADAR INDIA (Feb. 22, 2016, 3:34 PM), http://www.in.techradar.com/news/internet/The-reach-of-ISISdwindling-on-Twitter/articleshow/51090888.cms [http://perma.cc/5ZD9-K8CS].

116. Complaint, *supra* note 64, at ¶ 43.

117. Yoree Koh, *Lawsuit Blames Twitter for ISIS Terrorist Attack*, WALL ST. J. (Jan. 14,

Additionally, Twitter has consistently rebuffed requests from the United States government and other governments to remove suspected terrorist accounts.[119] Under the current reading of the statute, if Twitter took the position, whether because of its self-proclaimed position as a steward of free speech or otherwise, that it would not remove accounts identified by the United States government as DFTOs, this "deliberate indifference"[120] would likely satisfy the mens rea requirement.[121] For example, if the government identifies an account suspected to be run by ISIS and Twitter elects to keep the account open (as it has done in the past), it is openly providing material support to a group the government has just identified as a DFTO. Less clear is whether Twitter's policy of responding to reports instead of proactively monitoring its site for terrorist users satisfies the mens rea requirement on its own.[122]

In cases where the government has not done the work of identifying the accounts run by a DFTO—which is likely to be the majority of the time—the social media company is catapulted into the precarious position of defending whatever steps it has taken to identify and combat the use of its platform by terrorists as *enough*.[123] Worse, it potentially puts these

---

2016, 5:11 PM), http://blogs.wsj.com/digits/2016/01/14/lawsuit-blames-twitter-for-isis-terrorist-attack/ (last visited Sept. 28, 2016) (stating that Twitter does not actively police content except for images of child-sexual exploitation); *'Twitter Does Not Pro-actively Alert Authorities to Terrorist Content'*, ASIAN IMAGE (Feb. 2, 2016), http://www.asianimage.co.uk/news/14248369._Twitter_does_not_pro_actively_alert_authorities_to_terrorist_content_/ [http://perma.cc/YT7V-K6M9] (Twitter's UK public policy manager, Nick Pickles, is quoted as saying that the microblogging platform does not actively notify law enforcement for terrorist material found by staff or users).

118. Koh, *supra* note 117.

119. *See generally* Complaint, *supra* note 64, at ¶¶ 69–71.

120. *Boim II*, 549 F.3d at 692–93.

121. *See* Global-Tech Appliances, Inc. v. SEB S.A., 563 U.S. 754, 768 (2011) (The Supreme Court recently addressed the issue of willful blindness in a civil case for induced patent infringement. For the eight-justice majority, Justice Alito wrote: "Given the long history of willful blindness and its wide acceptance in the Federal Judiciary, we can see no reason why the doctrine should not apply in civil lawsuits . . . .").

122. Does waiting for third-parties to report abuse count as deliberate indifference? Another unanswered question.

123. Whether its efforts are enough is not likely to be decided on a Rule 12 motion.

companies in the position of determining who terrorists are and which accounts they own, something that is increasingly challenging given complaints from a global range based on different definitions of terrorism.

Additionally, most social media companies have terms of service and/or community guidelines that users must agree to in order to use the services.[124] These rules generally prohibit threatening speech, bullying, illegal conduct, and similar conduct.[125] Twitter's rules, for example, prohibit terrorist-driven content.[126] Facebook claims that any profile, page, or group related to a terrorist organization will be shut down and any content celebrating terrorism immediately removed.[127]

Any social media company with such a policy could argue that it has taken a stand against terrorists using its platform by virtue of its policy. But importantly, the company retains the exclusive right to decide how to enforce its rules, if at all.[128] In Twitter's case, where it prohibits terrorist-driven content, it alone has the power to define what "promoting terrorism" actually means.[129] However, simply posting a set of rules "banning" terrorists from exploiting their sites where there is little or no follow-up

---

124. *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK (Jan. 30, 2015), http://www.facebook.com/terms [http://perma.cc/B28X-WS24].

125. *See, e.g.*, *Statement of Rights and Responsibilities*, *supra* note 124 ("You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence."); *The Twitter Rules*, TWITTER (2016), http://support.twitter.com/articles/18311# [http://perma.cc/VQ5Y-X7ZD] ("You may not make threats of violence or promote violence, including threatening or promoting terrorism.").

126. *See The Twitter Rules*, *supra* note 125 ("Violent threats (direct or indirect): You may not make threats of violence or promote violence, including threatening or promoting terrorism," "Hateful conduct: You may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease. We also do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories.") (emphasis added).

127. Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015, 7:00 AM), http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/ [http://perma.cc/6ZV5-QDBL].

128. *Twitter Terms of Service (If You Live in the United States)*, TWITTER, http://twitter.com/tos?lang=en [http://perma.cc/AY4H-ZKFT].

129. The complaint against Twitter by Ms. Fields thus smartly asserts that Twitter enforced its rules only after it was notified of their violation and that it did not take enough of a proactive role in discovering abuses—and potentially defining certain uses as abuses. Complaint, *supra* note 64, at 10–11.

regarding compliance is not enough to disclaim knowledge under the ATA.

Exactly how diligent social media has to be to escape knowledge is not clear. As one commentator asked: "Does a tweet promote terrorism if it comes from an account kept by known terrorists? What constitutes a threatening tweet? And perhaps most important, how does Twitter decide who is a terrorist? Does Twitter have the sophistication necessary to make these judgments across the world amid constantly shifting cultural norms and complex political upheavals?"[130] Is taking down 125,000 accounts evidence that Twitter[131] is policing sufficiently? What if Twitter knew or, even murkier, suspected of 300,000 accounts? 1,000,000? Establishing the threshold of what is "enough" is a fact-driven question that could too easily leave Twitter on the wrong side of the line.

After Ms. Fields filed suit, Twitter claimed in a blog post that it would aggressively address terrorists' exploitation of its platform. "We have increased the size of the teams that review reports, reducing our response time significantly. We also look into other accounts similar to those reported and leverage proprietary spam-fighting tools to surface other potentially violating accounts for review by our agents. We have already seen results, including an increase in account suspensions and this type of activity shifting off of Twitter."[132] Twitter went on to say that:

> Violent threats and the promotion of terrorism deserve no place on Twitter and, like other social networks, our rules make that clear. We have teams around the world actively investigating reports of rule violations, identifying violating conduct, partnering with organizations countering extremist content online, and working with law enforcement entities when appropriate.[133]

Twitter's position thus far seems to be that it will make efforts to both identify and remove accounts when it knows an account is being operated

---

130. Jessi Hempel, *Twitter's Latest Challenge: Deciding Who's a Terrorist*, WIRED (Jan. 8, 2016, 7:00 AM), http://www.wired.com/2016/01/twitters-latest-challenge-is-deciding-whos-a-terrorist/ [http://perma.cc/HFX9-JRPZ].

131. This applies to all social media platforms as well.

132. Twitter, *supra* note 111.

133. *Id.*

by a terrorist organization. But should the obligation be on Twitter to identify theses accounts in the first instance? Why not leave this burden on the government to identify terrorist organizations?

It is hard to know who is in the better position of being able to do so from a technological standpoint. Twitter has acknowledged that there "is no 'magic algorithm' for identifying terrorist content on the Internet, so global online platforms are forced to make challenging judgement [sic] calls based on very limited information and guidance."[134] Perhaps the government's recent outreach to partner with Silicon Valley to combat ISIS underscores that *policing* accounts is best approached as a joint effort.[135]

From a policy perspective, these efforts articulated by Twitter should be enough to highlight that it is not deliberately indifferent to the exploitation of its platform by terrorist organizations.[136] Facebook's more aggressive approach to combating the use of its site by terrorists—particularly in light of the fact that those measures were in place before it was a defendant in a material support case—shows the same.

Social media can and should be a leader in developing technology to assist in identifying suspicious accounts. But it does not follow that it should be required to catch and shut down each one. Such a standard would prove impossible to satisfy.

Causation: does social media need to foresee terrorism as a consequence?

Though courts generally agree that the "by reason of" language does not require a plaintiff to prove but-for causation,[137] there is a circuit split

---

134. *Id.*

135. McLaughlin, *supra* note 60.

136. The exception would be where the government has alerted it to a DFTO. In such a case, it would be hard to argue that the social media was reluctant to shut down such an account (unless its own in-depth internal investigation gave it a strong reason to oppose the request). Again, this is complicated by the varying definitions of "terrorism" used by different governments around the globe and their varying incentives for shutting down accounts. It would seem that, at a minimum, the social media company should engage in some due diligence with respect to a shut-down request, even if it made the decision to keep the account open.

137. Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 507 (E.D.N.Y. 2012) (noting that a "but for" cause cannot be required in the section 2333(a) context); Linde v. Arab Bank, PLC, 97 F. Supp. 3d 287, 323 (E.D.N.Y. 2015) (holding that "requiring 'but for' causation would effectively annul the civil liability provisions of the ATA").

regarding what exactly must be proven.[138] The Second Circuit requires proximate causation, compelling plaintiffs to establish a sufficient basis to believe the material support proximately caused the attack.[139] In other words, the terrorist attack must be a foreseeable consequence of the specific act of support and not simply a general risk of providing the service. The Seventh Circuit has a more lenient requirement.[140] Under its standard, a plaintiff has to prove only that there was a substantial probability that the social media site's provision of services was a contributing cause of the attack.[141] This is a remarkably broad theory of causation which could "potentially expose every Internet service provider to liability for horrible crimes committed anywhere in the world, not only by their users but even by individuals who were loosely affiliated with or even just inspired by those users."[142] The Ninth Circuit, where the Fields's and Gonzalez's suits against social media were filed, has yet to answer this question.

In the case brought by Ms. Fields, Twitter predictably argued that proximate causation is the appropriate standard. Twitter contended that the Second Circuit was correct and that the Seventh Circuit "ignored the language Congress chose in crafting the statute" when it interpreted the statute as requiring less than proximate cause.[143] Even though it is in Twitter's best interest to have this higher standard applied, courts have acknowledged that applying proximate causation in ATA material support

---

138. *See generally* Rothstein v. UBS AG, 708 F.3d 82 (2d Cir. 2013); *Boim II*, 549 F.3d 685.

139. *Rothstein*, 708 F.3d at 95 (2d Cir. 2013) ("[I]f, in creating civil liability through § 2333, Congress had intended to allow recovery upon a showing lower than proximate cause, we think it either would have so stated expressly or would at least have chosen language that had not commonly been interpreted to require proximate cause for the prior 100 years.").

140. *Boim II*, 549 F.3d at 695–700.

141. *Gill*, 893 F. Supp. 2d at 507 (noting that under the Seventh Circuit's standard, "because money is fungible, a defendant's provision of assistance to a terrorist organization does not have to be either a necessary or sufficient cause of the harm suffered by an ATA plaintiff or an ATA plaintiff's decedent in order for a section 2333(a) plaintiff to recover.").

142. Defendant Twitter, Inc.'s Motion to Dismiss at 22, Fields v. Twitter, Inc., No. 3:16-cv-00213-WHO (N.D. Cal. Mar. 10, 2016).

143. *Id.* at 20 n.6.

claims is complicated and is not necessarily a win for defendants.[144] Even assuming the Ninth Circuit adopted the proximate causation standard, the outcome may not necessarily be favorable to social media platforms, particularly in a case with a strong set of facts.[145]

Under a proximate causation standard, defendants are generally "liable only for those injuries that might have reasonably been anticipated as a natural consequence of the defendant's actions."[146] For a social media platform to be liable in a civil action brought under this statute, the resultant terrorist attack must have been a foreseeable consequence of allowing the terrorists to use its services to assist in some way with the attack. For example, in the actions brought by Ms. Fields and Mr. Gonzalez, the plaintiffs would be required to prove that social media could have reasonably anticipated that ISIS's use of its services to recruit, organize, and fundraise would result in the attacks on Nohemi and Carl. Social media's response has been that the allegations fail to draw a connection between the attacks and any specific tweets.[147] In the case brought by Ms. Fields, Twitter argued that "not even the thinnest of reeds connects [it] to this terrible event,"[148] contending that its "sole alleged connection to this controversy is that, among the hundreds of millions of individuals around the world who disseminate information to one another via the Twitter platform, there are some people affiliated with, or supportive of, ISIS who allegedly used the platform to transmit information for purposes of promoting ISIS's terrorist activities and agenda."[149] Indeed, as argued in Twitter's Motion to Dismiss:

> The Complaint makes no attempt to connect Twitter directly to Abu Zaid or his attack. It does not allege that ISIS recruited Abu

144. *See Gill*, 893 F. Supp. 2d at 507 (providing an in-depth analysis).

145. This idea will be further discussed in Section III, *infra*.

146. Boim v. Quranic Literacy Inst. & Holy Land Found. for Relief & Dev. (*Boim I*), 291 F.3d 1000, 1012 (7th Cir. 2002); *see also* Abecassis v. Wyatt, 704 F. Supp. 2d 623, 665 (S.D. Tex. 2010).

147. Defendant Twitter, Inc.'s Motion to Dismiss, *supra* note 142, at 1.

148. *Id.* at 2.

149. *Id.* at 4 (citation omitted).

> Zaid over the Twitter platform. Nor does it allege that Abu Zaid or ISIS used the Twitter platform to plan, carry out, or raise money for the attack. It does not even allege that Abu Zaid had a Twitter account or ever accessed the Twitter platform. And although the Complaint devotes considerable attention to how other terrorists allegedly used the Twitter platform, it never explains how that alleged use had even the remotest connection to Abu Zaid's 'lone wolf' attack.[150]

Ms. Fields suggested that it "was foreseeable that giving ISIS unfettered access to Twitter accounts would enable them to recruit, fundraise, and spread their propaganda and that this would lead to the deaths of innocent civilians."[151] This argument, however, does not rise to the level of causation required by a proximate causation standard because there must be a tighter link between the act of support and the terrorist event. A stronger argument may have been that ISIS's use of social media incited this lone wolf attack, but that too would likely fail if the Ninth Circuit uses the proximate causation standard.

An easier road for plaintiffs would be under the substantial probability standard. Should the Ninth Circuit adopt the Seventh Circuit's substantial probability standard, plaintiffs like Ms. Fields and Mr. Gonzalez would only need to prove that there was a substantial probability that the provision of services by social media was a contributing cause of the attack. For example, Ms. Fields or Mr. Gonzalez could meet this standard if they could uncover additional information during discovery about Twitter's resistance to government efforts to combat terrorism via monitoring and removal of suspected terrorist accounts. This is regardless of whether ISIS's use of Twitter incited the lone wolf to attack or whether the attack was carried out on behalf of ISIS. This type of standard shifts the risk to social media platforms where there is a strong likelihood that harm will flow from the provision of services to terrorists.

---

150. *Id.* at 5.

151. Mark Sullivan, *How Twitter Will Win Lawsuit Brought By Woman Widowed By ISIS*, FAST COMPANY (Jan. 20, 2016, 3:45 PM), http://www.fastcompany.com/3055539/how-twitter-will-win-the-lawsuit-brought-by-the-woman-widowed-by-isis [http://perma.cc/F78N-XSY5].

3. What standard should the Ninth Circuit adopt?

The Ninth Circuit should follow the Second Circuit and adopt a proximate causation standard in material support cases. The words "by reason of" suggest it is the appropriate standard. The Supreme Court has interpreted identical language to require a showing of proximate cause.[152] Despite the interpretation of the Seventh Circuit to the contrary, most other courts considering the issue have held that the ATA contemplates a requirement of proximate causation.[153] District courts in the Second Circuit considering this issue came to that conclusion[154] long before the Second Circuit rubber-stamped that approach.[155] District courts from the D.C. Circuit and the Fifth Circuit agree.[156] Additionally, before reversing its position following an en banc hearing, the Seventh Circuit originally interpreted the ATA to require a finding of proximate cause. As the Second Circuit explained, the "by reason of" language has a "well-understood meaning" and that meaning does not "permit recovery on a showing of less than proximate cause, as the term is ordinarily used."[157] Indeed, in considering the interpretation of the same language, albeit in a different context, the Supreme Court explained that it has long construed those words to require proof of proximate cause.[158]

This interpretation makes sense. Proximate causation balances

---

152. *See* Holmes v. Sec. Investor Prot. Corp., 503 U.S. 258, 265–68 (1992) (interpreting "by reason of" language in civil RICO provision to require a showing that the defendant's conduct proximately caused the plaintiff's injury).

153. *E.g.*, Rothstein v. UBS AG, 708 F.3d 82, 95 (2d Cir. 2013).

154. Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 507–08 (E.D.N.Y. 2012); Strauss v. Credit Lyonnais, S.A., No. CV-06-0702 (CPS), 2006 WL 2862704, at *17 (E.D.N.Y. Oct. 5, 2006); Stutts v. De Dietrich Grp., No. 03-CV-4058 (ILG), 2006 WL 1867060, at *3, *4 (E.D.N.Y. June 30, 2006).

155. *Rothstein*, 708 F.3d at 95.

156. Abecassis v. Wyatt, 704 F. Supp. 2d 623, 665 (S.D. Tex. 2010); Kilburn v. Socialist People's Libyan Arab Jamahiriya, 376 F.3d 1123, 1128 (D.C. Cir. 2004); *see* Sisso v. Islamic Republic of Iran, No. 05-0394 (JDB), 2007 WL 2007582, at *11 (D. D.C. July 5, 2007).

157. *Rothstein*, 708 F.3d at 95.

158. *See* Holmes v. Sec. Investor Prot. Corp., 503 U.S. 258, 268 (1992) (interpreting the same language in a civil RICO case).

accountability with foreseeability: it requires that the defendant's conduct was a "substantial factor" in the injury and that the injury was "reasonably foreseeable" as a natural consequence.[159] Such a requirement protects against concerns that "civil liability could be extended to a potentially endless class of groups and individuals that provide even the most remote support to a terrorist group"[160] and that "it will lead to perpetual liability for all future attacks conducted by the terrorist group."[161] This approach is fair: unless there is a sufficient nexus to connect the usage of the social media platform to the injury-causing event, liability cannot exist.

Even under this standard, however, social media is not off the hook. These companies would have cause for concern if a DFTO tweets, posts, blogs, or otherwise uses social media to communicate about a forthcoming attack with some level of detail so that a victim of that attack could draw a direct connection between the service and the injury. Terrorists do this all the time. ISIS has already used Twitter to send messages to United States citizens, warning that they will be targets of ISIS.[162] After President Obama authorized military airstrikes against ISIS in Iraq, one tweet warned: "if America attacks #Iraq; every American embassy in the world will be exposed and attacked with car bombs."[163] A victim injured in an ISIS attack on an embassy would satisfy the proximate causation requirement with that mere tweet. It is also possible that causation would be met where a lone wolf attacker was radicalized online via a terrorist's social media accounts.

Social media would also be on the hook for causation where it has

---

159. *Boim I*, 291 F.3d at 1012 (explaining that the most common test of proximate cause is foreseeability and that defendants in tort actions are generally "liable only for those injuries that might have reasonably been anticipated as a natural consequence of the defendant's actions"); *see also Abecassis*, 704 F. Supp. 2d at 659.

160. Budoff, *supra* note 69.

161. *Id.* at 1083.

162. *See* David Martosko, *'A Message from ISIS to the US': Islamist Militants Tweet Gruesome Images of Dead American Soldiers and Vow to Blow Up Embassies as Terrorist Convoy is Wiped Out in Second Round of Airstrikes*, DAILY MAIL (Aug. 9, 2014, 8:49 PM), http://www.dailymail.co.uk/news/article-2720309/AmessagefromISIStoUS-Islamist-militants-tweet-gruesome-images-dead-American-soldiers-vow-blow-embassies-Obama-launches-airstrikes.html (last visited Sept. 28, 2016).

163. *Id.*

allowed terrorists to buy and sell weapons through its site. "A terrorist hoping to buy an antiaircraft weapon in recent years needed to look no further than Facebook."[164] An April 2016 study by Armament Research Services, a private consultancy group, along with an investigation by the New York Times, revealed that Facebook has "been hosting sprawling online arms bazaars, offering weapons ranging from handguns and grenades to heavy machine guns and guided missiles."[165] These bazaars appeared "in regions where the Islamic State has its strongest presence."[166] Using Facebook's closed groups and private messaging, sales could be arranged and transactions executed.

Such sales and solicitations violate Facebook's policies, which since January 2016 forbid the private sales of guns and ammunition.[167] However, it is unclear how involved Facebook is with enforcing this policy. One commentator suggested that "Facebook continues to host a bustling arms marketplace, where everything from handguns to rifles are easy to procure, often without a background check."[168] A material support claim against Facebook where the causal link was an arms sale would clearly satisfy this causation requirement.

---

164. C.J. Chivers, *Facebook Groups Act as Weapons Bazaars for Militias*, N.Y. TIMES (Apr. 6, 2016), http://www.nytimes.com/2016/04/07/world/middleeast/facebook-weapons-syria-libya-iraq.html.

165. *Id. See generally* N. R. Jenzen-Jones & Graeme Rice, *The Online Trade of Light Weapons in Libya*, SANA DISPATCHES 1 (Apr. 2016), http://www.smallarmssurvey.org/fileadmin/docs/R-SANA/SANA-Dispatch6-Online-trade.pdf [http://perma.cc/5XU7-X9K9].

166. Chivers, *supra* note 164. *See generally* Jenzen-Jones & Rice, *supra* note 165, at 2.

167. *See* Chivers, *supra* note 164.

168. Bryan Schatz & Alexander Sammon, *Facebook's Ban on Gun Sales is Being Enforced by a Few Dedicated Users*, MOTHER JONES (June 27, 2016, 6:00 AM), http://www.motherjones.com/politics/2016/06/gun-sales-facebook-flagged-reported [http://perma.cc/9LFT-RX6F].

B. *Other Arguments Against Liability for Social Media*

There are several policy reasons supporting a discharge of liability for social media in material support cases.

1. Independent advocacy is not service.

The most intuitive response to lawsuits attempting to hold social media liable for terrorist acts is that it is unjust to penalize those companies for acts of terrorism when they have simply created communication platforms available to everyone in the world with an Internet connection. In other words, social media did not create its respective platforms to give a voice or support to terrorist organizations and further did not offer the services at terrorist's requests. While much of this argument is addressed with respect to the mens rea element, social media might have a secondary argument that to meet the definition of "service" as required by the ATA, it would have needed to do something at the command of the terrorist organizations.

In 2010, the Supreme Court distinguished between conduct in coordination with or at the direction of a terrorist group, which the statute prohibits, and wholly independent advocacy or activity that might benefit the group, which the Constitution protects.[169] The Humanitarian Law Project ("HLP"), a nongovernmental organization, sought to help the Kurdistan Workers' Party in Turkey and Sri Lanka's Liberation Tigers of Tamil Eelam (both DFTOs) learn how to peacefully resolve conflicts.[170] It recognized that this assistance fit the material support definitions of "training," "expert advice or assistance," "service," and "personnel" despite the fact that the support was in the form of speech and therefore challenged the constitutionality of the ATA.[171] The Supreme Court held that it did not matter that the HLP's support was speech:

> Given the sensitive interests in national security and foreign affairs at stake, the political branches have adequately

169. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 24 (2010).

170. *See id.* at 14–15.

171. *See id.* at 21–22 (arguing that the statute was unconstitutionally vague, as will be discussed further in Section III).

> substantiated their determination that, to serve the Government's interest in preventing terrorism, it was necessary to prohibit providing material support in the form of training, expert advice, personnel, and services to foreign terrorist groups, even assuming the supporters meant to promote only the groups' non-violent ends.[172]

It did matter, however, that the support was more than just independent advocacy. The Court drew a line and held that "service" under the ATA contemplated more than independent activity: it required concerted activity.[173] Chief Justice Roberts wrote for the Court: "Context confirms that ordinary meaning here. The statute prohibits providing a service 'to a foreign terrorist organization' . . . . The use of the word 'to' indicates a connection between the service and the foreign group."[174] Social media platforms would therefore have a strong argument that despite having general knowledge that terrorist groups used their services, they cannot be liable under the statute because their activity in providing the platform was performed wholly independent of any terrorist group.

This argument has not been raised yet in the pending cases against social media.[175] This is possibly because each defendant's Terms of Service define the services it provides users in such a way as to connect the services to the recipient. This definition is "fully consistent with Roberts' interpretation of precisely what the statute forbids."[176] Yet the argument is still compelling as there is something unsettling about finding social media liable for failing to exclude DFTOs from a service available to anyone.

---

172. *Id.* at 36.

173. *Id.* at 4 ("Independently advocating for a cause is different from the prohibited act of providing a service 'to a foreign terrorist organization.'").

174. *Id.* at 24.

175. Zoe Bedell & Benjamin Wittes, *Tweeting Terrorists, Part II: Does it Violate the Law for Twitter to Let Terrorist Groups Have Accounts?*, LAWFARE (Feb. 14, 2016, 6:35 PM), http://www.lawfareblog.com/tweeting-terrorists-part-ii-does-it-violate-law-twitter-let-terrorist-groups-have-accounts [http://perma.cc/N4CW-THVC].

176. *Id.*

2. The statute is vague as applied.

Social media could also argue that because it cannot know which users of its ubiquitous platforms are actually members of terrorist organizations, the statute is vague as applied. That was precisely the argument made by the HLP. It argued the statute did not provide adequate notice of what was prohibited, particularly as it related to the definitions of "training," "expert advice or assistance," "service," and "personnel."[177]

The Court rejected that challenge, distinguishing those terms from others that it had previously struck down as too vague, terms like "annoying" and "indecent."[178] It held that the term was conspicuous because Congress had added narrowing definitions to the statute over time, it provided clear, objective definitions of what constitutes support, and the definitions did not require "untethered, subjective judgments."[179] The Court acknowledged that the statute may not be clear in every case, but was clear enough for the HLP to recognize that its conduct "readily" fell into the common understanding of what those "vague" terms meant.[180] The HLP further argued that it would not be able to determine exactly how much direction or coordination would be necessary for an activity to constitute a "service" under the ATA.[181] For example, "Would any communication with any member be sufficient? With a leader? Must the 'relationship' have any formal elements, such as an employment or contractual relationship? What about a relationship through an intermediary?"[182] The Court dismissed those concerns as hypothetical because the HLP did not articulate "the degree to which *they* seek to coordinate their advocacy"[183] with the DFTOs and "instead described the

177. Holder v. Humanitarian Law Project, 561 U.S. 1, 19 (2010).

178. *Id.* at 20.

179. *Id.* at 21.

180. *Id.*

181. *See* Reply Brief for Conditional Cross-Petitioners at 5–9, Humanitarian Law Project v. Holder, 557 U.S. 966 (2009) (No. 09-89), 2009 WL 2904604, at *8.

182. *Holder*, 561 U.S. at 24.

183. *Id.* at 25.

form of their intended advocacy only in the most general terms."[184]

The same may not be true when it comes to social media. The concern that social media is knowingly providing a service under the statute is not merely hypothetical. Gabe Rottman of the ACLU has suggested social media has a credible argument that "in the context of providing 'communications equipment,' one could argue that the 'service' has to be something like renting a satellite phone (not passively providing data and hosting services)."[185] Whether this argument has legs is unclear, but there are strong policy reasons to support a definition that contemplates more than passively providing data and hosting services. A broad definition exposes just about any provider of web-based services to liability. Under such a broad definition, it is not clear where to draw the line. David Cole, who argued on behalf of the Humanitarian Law Project, underscores just how broad this interpretation is:

> What about Google, Facebook, or Verizon, all of which have almost certainly provided their "services," in the form of Google searches, social networking, and phone and email access, to Hamas or its members. For that matter, what about Pepsi and Coca-Cola, who have surely sold soda bottles to Hamas in the Gaza Strip? What about ExxonMobil and Shell Oil, whose gas has very likely powered Hamas vehicles? And what about public radio and CNN, whose news services are available around the world, including in Gaza?[186]

The Court did suggest that such a far-reaching application of the ATA would be frustrated by the "knowledge requirement of the statute [which] reduces any potential for vagueness,"[187] but Cole's frustration with the broad scope of the Court's interpretation is well-founded.

This is not to ignore policy implications of a broader definition—that

---

184. *Id.*

185. Gabe Rottman, *Hamas, Twitter and the First Amendment*, ACLU: FREE FUTURE (Nov. 21, 2012, 3:25 PM), http://www.aclu.org/blog/hamas-twitter-and-first-amendment [http://perma.cc/WDF9-W6XS].

186. Cole, *supra* note 88.

187. *Holder*, 561 U.S. at 21.

the goal of shutting down terrorist networks justifies a wide net—but it does suggest that there is a viable argument for vagueness as applied to the social media defendants and certainly others who are similarly situated.

IV. CAN SECTION 230 SAVE SOCIAL MEDIA?

In the present cases against social media, the facts weigh in the defendant's favor—neither plaintiff has alleged a strong causal link between activity on Twitter, Facebook, or YouTube (Google) and the attack. But even assuming the present complaints were both dismissed, social media still has reason for concern. The persuasive arguments against a causal link in these cases will not be true of every future litigant.[188] Moreover, a plaintiff in the Seventh Circuit would face a lower causation burden so even on a weak causal link, a case may proceed and even succeed against social media.[189] Instead, it would benefit social media to have the cases dismissed because the claims were legally untenable, *not* because the facts were not strong enough. Given the broad interpretation of the ATA by courts, coupled with the government's priority to attack terrorism from every angle,[190] it is unlikely for a court to find *as a matter of law* that social media could not be held liable under the ATA under any set of facts. However, a different statute could offer an answer.

Section 230 of the Communications Decency Act ("Section 230") protects Internet providers from liability for content posted on their sites by third parties.[191] To encourage companies to set up platforms where people can speak openly, section 230 provides that an interactive computer service (broadly defined to include a variety of websites, including social media platforms) cannot be treated as the publisher or speaker of third party content.[192] Simply put, section 230 protects social media sites, among

188. Recall the earlier hypothetical where a terrorist group tweets about a forthcoming attack with some level of detail so that a victim of that attack can draw a direct connection between the service and the injury. Or when an attack happens and the weapons used can be traced to a purchase via Facebook messenger.

189. *See, e.g.*, *Boim II*, 549 F.3d at 685.

190. Arguably at the expense of free speech on occasion.

191. 47 U.S.C. § 230(c) (2012).

192. *Id.* § 230(c)(1), (f)(2).

others, from civil liability for publishing content such as posts, pages, comments, tweets, etcetera generated by its users.

A recent case from the District of Columbia Circuit provides a helpful example. In *Klayman v. Zuckerberg*, the plaintiff alleged claims against Facebook for failing to promptly take down a page on its site entitled "Third Palestinian Intifada."[193] The page was created by users and called for Muslims to rise up and kill Jewish people.[194] The district court dismissed the claim, holding that section 230 shielded Facebook from liability because (1) it qualified as an interactive computer service; (2) the content was provided by third parties; and (3) the plaintiff attempted to treat Facebook as the publisher of the offending content.[195]

When the first case against social media based on the ATA was filed in January, the immediate reaction of several commentators was that section 230 was clearly applicable and would shield Twitter from liability.[196] But its application here is uncertain because as will be discussed below, whether section 230 affords immunity hinges upon whether the plaintiff is attempting to treat the defendant as the *publisher* of information posted by third parties. Here, the theory of liability against social media is not based on the content posted on its sites by terrorists, but instead on the *consequences* of allowing terrorists to use those services. In other words, social media is not being sued as the publisher or speaker of objectionable content, which are the types of claims section 230 guards against.

---

193. Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014).

194. *Id.*

195. *Id.* at 1357–59.

196. *See, e.g.*, Grant Burningham, *The Twitter Revolution Meets ISIS*, NEWSWEEK (Jan. 26, 2016, 2:35 PM), http://www.newsweek.com/twitter-revolution-meets-isis-419877 [http://perma.cc/T9MY-TSHY]; David Kravets, *Twitter Provides Material Support to ISIS, Lawsuit Alleges*, ARS TECHNICA (Jan. 14, 2016, 10:43 AM), http://arstechnica.com/tech-policy/2016/01/twitter-provides-material-support-to-isis-lawsuit-alleges/ [http://perma.cc/8CEG-Z9WR]; Jeff John Roberts, *Twitter Sued by Widow of ISIS Victim*, FORTUNE (Jan. 14, 2016, 12:04 PM), http://fortune.com/2016/01/14/twitter-isis-lawsuit/ [http://perma.cc/S7ZD-VCYJ]; Mark Sullivan, *How Twitter Will Win Lawsuit Brought By Woman Widowed By ISIS*, FAST COMPANY (Jan. 20, 2016, 3:45 PM), http://www.fastcompany.com/3055539/how-twitter-will-win-the-lawsuit-brought-by-the-woman-widowed-by-isis [http://perma.cc/F78N-XSY5].

A. *A Closer Look at the Contours of Section 230 Immunity*

Twenty years ago, Congress passed the Communications Decency Act to control and limit the exposure of children to indecent and obscene material online.[197] As perhaps a concession to the Internet industry, which was up in arms about the Act, section 230 was tacked on to address the growing concern that websites could be liable for content posted by third parties.[198] The following year, the Supreme Court struck down most of the Act as unconstitutional, leaving only section 230 intact.[199] Since that time, section 230 has evolved into what many commentators consider to be "one of the most valuable tools for protecting freedom of expression and innovation on the Internet."[200]

When it included section 230 as part of the Act, Congress recognized that the Internet "represent[ed] an extraordinary advance in the availability of educational and informational resources" and "offer[ed] a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[201] More importantly, the Internet was flourishing "with a minimum of government regulation."[202] Thus, Congress made it the "policy of the United States" to "promote the continued development of the Internet" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation[.]"[203]

---

197. *See generally* 47 U.S.C. § 223 (2012) (held unconstitutional by Reno v. ACLU, 521 U.S. 844 (1997)).

198. *CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/cda230/legislative-history [http://perma.cc/PHN9-8NW4] ("Worried about the future of free speech online and responding directly to *Stratton Oakmont*, Representatives Chris Cox (R-CA) and Ron Wyden (D-OR) introduced an amendment to the Communications Decency Act that would end up becoming Section 230.").

199. *See generally* Reno v. ACLU, 521 U.S. 844 (1997).

200. *CDA 230: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/cda230 [http://perma.cc/CA3G-EH3L].

201. 47 U.S.C. § 230(a)(1), (a)(3) (1998).

202. *Id.* § 230(a)(4).

203. *Id.* § 230(b)(1)–(4) (stating "(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the

The result is that section 230 commands that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" and "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[204] Interactive computer services are broadly defined to include not only traditional Internet Service Providers ("ISPs"), which are common carriers such as AT&T, Verizon, or Time Warner, but also a range of interactive computer service providers, which includes basically any online service that publishes third party content.[205] Thus, section 230 prohibits claims that treat websites as the "publisher" of third party content, regardless of whether the website exercised a traditional editorial function in reviewing, editing, or deciding whether to publish or to withdraw from publication any content created by users of its service.[206]

Since its inception, section 230 has protected websites such as Facebook, Google, Yahoo!, Craigslist, and others from liability stemming from the content posted on their sites by users, whether or not the respective website tried to block, remove, or police that content.[207] Of course, the third parties who created and posted the illegal material are not immune from liability.[208]

---

vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation; (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services; [and] (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . .").

204. *Id.* § 230(c)(1), (e)(3).

205. *Id.* § 230(f)(2).

206. *Defamation: CDA Cases*, ELECTRONIC FRONTIER FOUNDATION: INTERNET LAW TREATISE (Mar. 27, 2013, 6:02 PM), http://ilt.eff.org/index.php/Defamation:_CDA_Cases#Exercise_of_Editorial_Functions [http://perma.cc/XXV9-KSQ7].

207. *See generally Klayman*, 753 F.3d 1354; Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Ct. App. 2002); Barnes v. Yahoo!, Inc. (*Barnes II*), 570 F.3d 1096 (9th Cir. 2009); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009).

208. *Gentry*, 121 Cal. Rptr. 2d at 703.

The rationale behind such sweeping immunity was that it would "encourage interactive computer services and users of such services to self-police the Internet for obscenity and other offensive material . . . ."[209] Prior to the Act, if a website attempted to moderate third party posts to remove obscene material, for example, it was treated as a publisher for liability purposes and could be held liable if it was unsuccessful in removing *all* such material. A website that did nothing, on the other hand, faced no liability because it had no involvement, either in the form of publication or removal, with the content.[210] Thus, Congress attempted to allay the concern that a website's efforts to remove objectionable content might expose it to liability even when trying to be a "good online citizen."[211] Providing immunity accomplished this goal. Considering the sheer volume of material that is posted to many websites on any given day, policing all of the content would prove impossible and so the natural response of social media in such a situation without section 230 would be to do nothing.

Because it was concerned with protecting children, this was not the outcome Congress wanted. In passing section 230 and allowing sites to voluntarily filter content, Congress spared social media platforms from the grim choice of either performing some content-editing to remove obscene and offensive material or policing no content at all.

B. *Limits of Section 230*

Though immunity under section 230 is far-reaching, it is not without limits. Immunity is not available when an interactive computer service provider is the party responsible, in whole or in part, for the creation or development of content. In those cases, a computer service provider will be deemed the "information content provider" and can be held liable for that content.[212]

The Act also expressly carves out immunity from federal criminal

---

209. Batzel v. Smith, 333 F.3d 1018, 1028 (9th Cir. 2003); *see also* 47 U.S.C. § 230(b) (1998).

210. *Batzel*, 333 F.3d at 1029.

211. *Id.*

212. *Carafano*, 339 F.3d at 1123 ("Under the statutory scheme, an 'interactive computer service' qualifies for immunity so long as it does not also function as an 'information content provider' for the portion of the statement or publication at issue.").

law, intellectual property law, and communications privacy law.[213] This means that when an interactive computer service provider itself violates a specific federal criminal law, for example, it will lose immunity under section 230[214] and the government can pursue charges against it.

Importantly, this does not translate into a loss of immunity against a civil suit based on the same conduct. Section 230 has continued to insulate providers against civil claims even when they are based on federal criminal statutes.[215] For example, the United States District Court for the Eastern District of Texas dismissed claims that Yahoo! was tortiously liable to victims of child pornography because it violated a federal criminal statute by knowingly profiting from the trafficking of child pornography.[216] Most other courts that have considered the issue are in accord with this policy.[217] Thus, even assuming Ms. Fields could show that Twitter violated the

213. 47 U.S.C. § 230(e)(1)–(3) (1998).

214. *Id.* § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of . . . [any] Federal criminal statute.").

215. *See, e.g.*, Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *5 (E.D. Tex. Dec. 27, 2006) (holding that section 230 immunity applied, even if Yahoo! knowingly profited from a site where members exchanged sexually explicit photographs of minors). *See generally* Doe v. MySpace, Inc. (*MySpace, Inc. I*), 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd*, Doe v. MySpace, Inc. (*MySpace, Inc. II*), 528 F.3d 413 (5th Cir. 2008) (holding that MySpace was entitled to immunity under section 230 against claims of a 14 year old who was sexually assaulted by a man she met on the site).

216. *Bates*, 2006 WL 3813758, at *5, *22 ("Congress decided not to allow private litigants to bring civil claims based on their own beliefs that a service provider's actions violated the criminal laws.").

217. *See, e.g.*, Obado v. Magedson, No. 13-2382 (JAP), 2014 WL 3778261, at *8 (D. N.J. July 31, 2014), *aff'd*, 612 F. App'x 90 (3d Cir. 2015) ("[T]he CDA exception for federal criminal statutes applies to government prosecutions, not to civil private rights of action . . . ."); GoDaddy.com, LLC v. Toups, 429 S.W.3d 752, 760 (Tex. App. 2014) (finding that section 230 affords interactive computer service providers immunity from civil liability even if the posted content is illegal or forms the basis of a criminal prosecution); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 965 n.6 (N.D. Ill. 2009) (holding that the complaint's reference to a criminal statute did not bring a nuisance cause of action within the statutory exception to CDA immunity provided under section 230(e)(1)). *See generally* M.A. ex rel. P.K. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041 (E.D. Miss. 2011) (the illegal or highly offensive nature of website content does not alter the controlling determination of whether the information was created by an information content provider other than the defendant). Two courts, the Eastern District in Missouri and the Seventh Circuit, have considered arguments that an ISP could lose section 230 immunity if it aided and abetted a crime. *See, e.g.*, Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

criminal provisions of the ATA, Twitter would have a very strong argument that if section 230 applied, it would bar her civil claim based on that violation of federal law.

C. *When Section 230 Applies and the Distinction Social Media Would Like to Avoid*

Three elements are required for section 230 immunity: (1) the defendant must be a provider or user of an "interactive computer service"; (2) the asserted claims must treat the defendant as a publisher or speaker of information; and (3) the challenged communication must be "information provided by another information content provider."[218]

Social media sites easily meet the first prong as they provide "interactive computer services."[219] For example, Twitter is an operator of an interactive website that allows users to send and read short 140-character messages called "tweets." [220] Facebook operates an interactive site that allows users to create profiles, post commentary, links, images, videos, and interact with other users both via private messages and public posts on other user's "walls."[221] YouTube offers a platform for uploading, viewing, sharing, and commenting on videos.[222]

The second and third prongs pose a challenge for social media platforms in cases where Plaintiffs assert material support claims against them. This is because section 230 is designed to protect services from being treated as the *publisher* of content posted by third parties. In cases against social media brought under the ATA, the claim made by plaintiffs is that the service is supporting terrorism by permitting terrorists to use its

---

218. *Obado*, 612 F. App'x at 4; Kabbaj v. Google, Inc., No. 13-1522-RGA, 2014 WL 1369864, at *2 (D. Del. Apr. 7, 2014); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007); Batzel v. Smith, 333 F.3d 1018, 1037 (9th Cir. 2003) (Gould, J., dissenting).

219. *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003); *see also* Beckman v. Match.com, No. 2:13-CV-97 (JCM NJK), 2013 WL 2355512, at *3 (D. Nev. May 29, 2013); Doe v. SexSearch.com, 502 F. Supp. 2d 719, 725 (N.D. Ohio 2007), *aff'd*, 551 F.3d 412 (6th Cir. 2008); *MySpace, Inc. II*, 528 F.3d at 418.

220. TWITTER, www.twitter.com [http://perma.cc/2BTK-ND62].

221. FACEBOOK, http://www.facebook.com [http://perma.cc/BMY8-ZAUX].

222. YOUTUBE, http://www.YouTube.com [http://perma.cc/2SS7-XWUH].

service. This is distinct from a claim that the social media site is liable for the content of a specific tweet or post made by a terrorist organization. The latter is the type of claim section 230 routinely guards against.

This distinction is exemplified by *Klayman v. Zuckerberg*, discussed *supra*, a case that Twitter relied upon in its Motion to Dismiss in the case brought by Ms. Fields.[223] Recall that in *Klayman*, the plaintiff's claims were based upon a Facebook page entitled "Third Palestinian Intifada," which called for Muslims to kill Jewish people.[224] After Plaintiff complained about the page, Facebook removed it, but not promptly enough for the Plaintiff.[225] He filed suit against Facebook and its founder, Mark Zuckerberg, alleging that their delay in removing that page and similar pages constituted intentional assault and negligence."[226] The distinction between *Klayman* and the claims brought under the ATA is critical: the plaintiff in *Klayman* alleged that Facebook was liable to him for content posted on its site by a third party, an allegation which section 230 expressly prevents. There was no allegation that Facebook violated the ATA or that the ATA was even at issue in the *Klayman* case. The cause of action was based on negligence and assault and liability was predicated on Facebook's status or conduct as a publisher. The plaintiff sought to hold Facebook liable for the exact conduct that section 230 prohibits and consequently, the Court properly dismissed the suit.[227]

Conversely, in the cases brought under the ATA, plaintiffs have argued that social media is liable not for the content posted online (which would be a direct analogy to *Klayman*), but instead for the *consequences* of

223. *See generally* Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014).

224. *Id.* at 1355.

225. *Id.*

226. *Id.*

227. *See*, *e.g.*, Zeran v. Am. Online, Inc. (*Zeran II*), 129 F.3d 327, 330 (4th Cir. 1997) (stating that the Communications Decency Act protects against liability for the "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content"); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 422 (1st Cir. 2007) (same); Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003) (same); Doe v. MySpace, Inc. (*MySpace, Inc. II*), 528 F.3d 413, 420 (5th Cir. 2008) (no liability under the Act for "decisions relating to the monitoring, screening, and deletion of content" by an interactive computer service provider) (quoting Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003)); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC., 521 F.3d 1157, 1170–71 (9th Cir. 2008*)* ("[A]ny activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230.").

allowing terrorists to use its services.[228] The lawsuits are not directed at specific, offensive content.[229] In the present actions, the defendants thus far have ignored this distinction, arguing instead that any liability based on the use of its platforms to spread propaganda, raise funds, and recruit followers, regardless of the effect, is barred by section 230.

V. SAVING SOCIAL MEDIA UNDER SECTION 230 COMPORTS WITH CONGRESSIONAL POLICY AND BROAD JUDICIAL INTERPRETATION

The application of section 230 to cases brought under the ATA may not be clear, but the impact of holding social media liable for terrorist acts certainly is. Every content provider that provides communication tools to its users would feel the sting if social media were held liable for terrorist acts. These content providers would be forced to fundamentally change the speech they allow and the way they interact with users, which would consequently chill speech. If Ms. Fields and Mr. Gonzalez or future plaintiffs are able to successfully premise liability on allowing terrorists to use social media, instead of premising liability on the harm flowing from specific posts, it will frustrate the very goals Congress sought to advance in enacting section 230.

A. *Congress Intended to Provide Robust Immunity Under Section 230*

The legislative history behind section 230 illustrates that Congress wanted to protect online intermediaries from liability in order to encourage the unfettered growth of the Internet:

> Congress reasoned that any liability would threaten development of the online industry as a medium for new forms of mass communication and simultaneously create disincentives to self-regulate such content by content providers. Congress therefore determined that liability should rest with the actual wrongdoers—the originators of the illegal and harmful content—and not intermediary servers whose systems are sometimes abused by

228. Complaint at ¶¶ 69–71, Fields v. Twitter, Inc., No. 4:16-CV-00213-KAW (N.D. Cal. filed Jan. 13, 2016); Verified Complaint at ¶¶ 1–2, Gonzalez v. Twitter, Inc., No. 3:16-cv-03282 (N.D. Cal. filed June 14, 2016).

229. Ironically, if they were, causation might not be as high a hurdle for the plaintiffs.

wrongdoers.[230]

The legislative history indicates that the overarching goal was to immunize "providers and users of interactive computer services for actions to restrict or to enable restriction of access to objectionable online material."[231]

Courts have given deference to this goal, broadly interpreting section 230 to immunize providers and users of ISPs from claims related to defamation, negligence, intentional infliction of emotional distress, privacy, and others.[232]

B. *A Broad Reading of Section 230 Would be Consistent with Judicial Interpretation of the Statute*

The seminal case interpreting section 230 immunity is *Zeran v. America Online, Inc.*[233] After the Oklahoma City bombing, the plaintiff discovered that someone had falsely advertised on America Online that he was selling T-shirts containing tasteless slogans about the attack.[234] As a result, the plaintiff received a "flood of abusive phone calls," which came as frequently as every two minutes, in addition to death threats[235] He sued, claiming that AOL "failed to remove the postings immediately, failed to notify other subscribers of the message's false nature and failed to

230. Barnes v. Yahoo!, Inc. (*Barnes I*), No. Civ. 05-926-AA, 2005 WL 3005602, at *2 (D. Or. Nov. 8, 2005).

231. H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.) (including the Conference Report from the House of Representatives dated January 31, 1996 as related to 47 U.S.C. § 230 (1998)).

232. *See*, *e.g.*, Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006) (claim under Maryland Commercial Electronic Mail Act); Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *5 (E.D. Tex. Dec. 27, 2006) (negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy and distribution of child pornography); *Barnes I*, 422 F. Supp. 2d, at *4 (negligence claim resulting in personal injury); Batzel v. Smith, 333 F.3d 1018, 1029 (9th Cir. 2003) (defamation); Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000) (negligence claim); Zeran v. Am. Online, Inc. (*Zeran II*), 129 F.3d 327, 330–31 (4th Cir. 1997) (negligence claims).

233. *Zeran II*, 129 F.3d at 331–33.

234. Zeran v. Am. Online, Inc. (*Zeran I*), 958 F. Supp. 1124, 1127 (E.D. Va. 1997).

235. *Id.* at 1128.

effectively screen future defamatory material."[236] The trial court dismissed the action and the Fourth Circuit affirmed, holding that immunity under section 230 is extended even when a provider is notified of objectionable content on its site.[237] *Zeran's* importance stems from the fact that not only was it one of the first cases to interpret section 230, but also because nearly every court to consider the issue since has relied on its decision.

Following *Zeran*, the Ninth Circuit has characterized immunity under section 230(c)(1) as "quite robust"[238] and other courts of appeal to consider the issue are in accord with this characterization.[239] Ultimately, this broad interpretation of section 230 is necessary to avoid a chilling effect on free speech. Faced with restricting speech of its users or facing liability, content providers would choose the former. In recognition of this, courts have applied section 230 to cover a variety of different claims. For example, immunity has been applied to a website that offered an "adult" services section that allegedly facilitated prostitution,[240] dating websites,[241] e-mail forwards,[242] links,[243] and countless others. The common thread uniting each case has been that the plaintiff tried to treat the content provider as the publisher of information from a third-party.

Over the past decade, a thread of cases has emerged against MySpace, another social networking website.[244] In each of these cases, minor females

---

236. Doe II v. MySpace Inc., 96 Cal. Rptr. 3d 148, 154 (Ct. App. 2009).

237. *Zeran II*, 129 F.3d at 330.

238. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC., 521 F.3d 1157, 1179 (9th Cir. 2008); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

239. Chi. Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670–71 (7th Cir. 2008); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 415 (1st Cir. 2007); Green v. Am. Online (AOL), 318 F.3d 465, 470 (3d Cir. 2003); Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000); *Zeran II*, 129 F.3d at 330.

240. Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 961 (N.D. Ill. 2009).

241. *See generally* Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262 (N.D. Cal. 2006).

242. Barrett v. Rosenthal, 146 P.3d 510, 514 (Cal. 2006); Mitan v. A. Neumann & Associates, LLC, No. 08-6154, 2010 WL 4782771, at *1 (D. N.J. Nov. 17, 2010).

243. Life Designs Ranch, Inc. v. Sommer, 364 P.3d 129, 138 (Wash. Ct. App. 2015).

244. MYSPACE, http://www.myspace.com [http://perma.cc/LY2R-G3YA].

brought claims against MySpace after they were sexually assaulted by men they met through the website.[245] Plaintiffs in these cases have predicated liability on the fact that section 230 was inapplicable because the lawsuit was not related to the publication of third-party content, but based on a failure to implement basic safety measures to prevent sexual predators from communicating with minors on MySpace.[246] This is exactly the argument in the present actions: plaintiffs allege that Twitter, Facebook, and Google are liable not for their publication of third-party content, but instead for harms that flow from their failure to prevent terrorists from using its site. A court interpreting the plain language of section 230 would likely recognize this distinction and thereby allow the claim to proceed. However, the opposite has been true.

Both the Fifth Circuit and the California Court of Appeals have interpreted the claims as directed towards MySpace's publishing, editorial, and/or screening capacity, despite the fact that plaintiffs pled harms stemming from its failure to exclude a certain type of user.[247] As the Court in *Doe II v. MySpace Inc.* explained:

> That appellants characterize their complaint as one for failure to adopt reasonable safety measures does not avoid the immunity granted by section 230. It is undeniable that appellants seek to hold MySpace responsible for the communications between the Julie Does and their assailants. *At its core, appellants want MySpace to regulate what appears on its Web site.* Appellants argue they do not "allege liability on account of MySpace's exercise of a publisher's traditional editorial functions, such as editing, altering, or deciding whether or not to publish certain material, which is the test for whether a claim treats a website as a publisher . . . ." But that is precisely what they allege; that is, they want MySpace to ensure that sexual predators do not gain access to (i.e., communicate with) minors on its Web site. That type of activity—to restrict or make available certain material—is expressly covered by section 230.[248]

245. *See generally* Doe II v. MySpace Inc., 96 Cal. Rptr. 3d 148, 154 (Ct. App. 2009) (consolidating four cases); *MySpace, Inc. I*, 474 F. Supp. 2d at 848.

246. *MySpace, Inc. I*, 474 F. Supp. 2d at 848.

247. *Id.*; *see also Doe II v. MySpace Inc.*, 96 Cal. Rptr. 3d 148.

248. *Doe II v. MySpace Inc.*, 96 Cal. Rptr. 3d at 156–57 (emphasis added).

It did not matter that plaintiffs tried to shift the focus to the resultant harm: "Plaintiffs' allegations that MySpace knew sexual predators were using the service to communicate with minors and failed to react appropriately can be analogized to Zeran's claims that AOL failed to act quickly enough to remove the ads and to prevent the posting of additional ads after AOL was on notice that the content was false."[249] Both courts ultimately held that the allegations were merely another way of claiming that MySpace was liable for publishing the communications, which was enough to trigger section 230 immunity.[250]

The analogy here is clear. Social media can make a strong argument that plaintiffs bringing claims under the ATA are attempting to skirt around section 230 by characterizing the claim as one based on the ability of terrorists to use their platforms, instead of one based on the content of the posts, videos, and/or tweets. However, in the end, this type of plaintiff is really premising liability on the fact that social media published information created by terrorists.

Even though Twitter ignored this distinction in its Motion to Dismiss in the *Fields* case, it laid some groundwork that could support such an argument.[251] In *Fields*, Twitter argued that the allegations that it failed to take "meaningful action to stop" terrorist use of its site by "censoring user content," "shutting down . . . ISIS-linked accounts," or blocking ISIS related accounts from "springing right back up" is "precisely the kind of activity for which Congress intended to grant absolution with the passage of section 230."[252]

It takes the argument too far to suggest that Congress intended to provide immunity to social media even when terrorists use it to spread propaganda, recruit, and fundraise. However, the first stated goal of the statute is "to promote the continued development of the Internet and other interactive computer services and other interactive media" and a dismissal

249. *Id.* at 156.

250. *Id.*; *MySpace, Inc. II*, 528 F.3d at 420.

251. *See generally* Defendant Twitter, Inc.'s Motion to Dismiss, Fields v. Twitter, Inc., No. 3:16-cv-00213-WHO (N.D. Cal. Mar. 10, 2016).

252. *Id.* at 15 ("Whatever theory or label Plaintiff invokes, 'such conduct is publishing conduct,' and '[S]ection 230 protects from liability any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online.'").

on section 230 grounds would further this goal.

C. *A Narrow Reading Could Frustrate Congress's Goals in Enacting Section 230*

If plaintiffs can successfully defeat a section 230 defense, the result could be dire for the technology industry. It would essentially stifle the development of any interactive service that seeks to provide an unmoderated service that is open to proliferating speech, which is exactly what section 230 sought to prevent. Recognizing this, in response to the case brought by Ms. Fields, Twitter made the policy argument that if it "were potentially subject to liability for every third-party communication, it would face enormous pressure to transform its open platform into a tightly restricted and heavily censored one—or to shut down altogether."[253] Aaron Mackey, a legal fellow at the Electronic Frontier Foundation, commented that: "It has the potential to escalate and require a lot of changes to technology companies, shutting off whole swaths of access to regions of the world and to types of people."[254] Indeed, if future plaintiffs bring ATA claims against social media and are successful, it would dramatically redefine "free speech" on social networks. Such a shift would impact not only the way social media reviews content, but also the very way these sites allow users to interact with one another, publish content immediately, and enjoy substantial freedom in postings.

VI. CONCLUSION

There can be no doubt that cutting off terrorist groups' ability to communicate, fundraise, and spread propaganda is critical to their defeat. But, premising liability on the basis that social media companies provide a platform for millions of people to use, *a fraction of whom are terrorists*, has grave consequences. These consequences extend not just to social media companies, but also to any web-based communication and support companies—essentially to any company that supplies any of the tools and instrumentalities DFTOs may use. The problem is particularly acute for social media companies, however, where the business model relies on the

253. *Id.* at 10.

254. Hamza Shaban, *Twitter Sued For Helping Explosive Growth of ISIS*, BUZZFEED NEWS (Jan. 15, 2016, 12:57 PM), http://www.buzzfeed.com/hamzashaban/lawsuit-blaming-twitter-for-isis-attack-draws-allegations-fr#.tyQkMAa8M [http://perma.cc/BL6E-AN3M].

company allowing its users the freedom to communicate with one another with little involvement, interaction, or oversight by the administrator. A finding of liability would fundamentally change the way these systems operate. The companies would be forced to take on not just a more active role, but a very proactive role in determining who its users are and monitoring suspicious posts. The ability to speak freely and without censure online would shrink and the very nature of social networking would dramatically change.

If the United States government can identify specific social media accounts used to further terrorist efforts, those platforms should work with the government to shut them down. However, it does not follow that social media and other web services should shoulder the burden of identifying all terrorists on their platforms or face civil liability for terror attacks.

This is particularly true where Congress has immunized content providers from liability for third-party posts to specifically promote the growth and development of the Internet. This policy is not in conflict with the policy of preventing terrorism—it is in conflict with *the award of civil liability for terrorist acts made by users of that service*. If courts choose to favor the latter policy, it does little to shut down terrorist networks. Instead, it changes the nature of social media platforms into highly censored or nonexistent forums of communication. Or worse, it shuts them down altogether, which is precisely what Congress sought to prevent with section 230. For this reason, claims under the ATA for civil liability against social media platforms predicated on allowing terrorists to use its services should be dismissed under section 230.