How Civil Aiding and Abetting Liability for Terrorist Activities Applies to Social Media Companies—And How it Does Not

Nathaniel Parr[†]

ABSTRACT

The 2023 Supreme Court case Twitter v. Taamneh *found that defendant social media companies were not liable for aiding and abetting a terrorist attack overseas. The Court alluded to the existence of an alternative set of facts that might alter their analysis or produce a different outcome. This Comment explores those "other contexts" and seeks to identify what factors could produce a successful Justice Against Sponsors of Terrorism Act (JASTA) aiding and abetting claim against a social media company for an act of terrorism overseas. This is difficult, in part, because the framework for aiding and abetting liability provided in JASTA is seemingly incompatible with the operations of social media companies. To better evaluate how JASTA's framework should apply to social media companies, both JASTA cases that do not involve social media companies and aiding and abetting cases derived from other sources are analyzed for their relevance to the social media context.*

Ultimately, this Comment concludes that it would take an extraordinary set of facts to find social media companies secondarily liable for an act of terrorism. This is, in part, due to the nature of how social media operates and continues to progress at a rapid pace. The increasing role that social media plays in society highlights why deterring further Foreign Terrorist Organization (FTO) use of social media is critical; as avenues to recruitment and international planning increase, the risk to the United States' national security also increases. Given that JASTA is not a solution, this Comment suggests other avenues to encourage social media companies to heighten their detection of FTO activity and prevent future attacks.

[†] B.S., Georgia Institute of Technology, 2018; M.S., Georgia Institute of Technology, 2019; J.D. Candidate, The University of Chicago Law School, 2025. I am deeply grateful for the guidance and wisdom imparted by Professor Genevieve Lakier which made this Comment possible. I also thank Caroline Kelly, whose mentorship has been instrumental during my time studying law.

I. INTRODUCTION

Since the terrorist attacks on the World Trade Center in New York on September 11, 2001, the United States government has placed an increased emphasis on preventing and deterring terrorist groups abroad. The goals and strategies of these terrorist groups are always evolving, and social media plays a growing role in their operations.[1] Yet it is unclear exactly how current law may punish and deter social media companies from inadvertently assisting international terrorist operations.

In the United States, victims of acts of international terrorism can seek civil recourse through the Anti-Terrorism Act (ATA).[2] As initially enacted, the ATA expressly provided recourse only for primary liability, meaning the defendant needed to have actively participated in the terrorist attack.[3] Courts disagreed over whether secondary liability claims, in which the defendant assisted the primary tortfeasor, were available under the ATA.[4] In 2016, Congress amended the ATA with the Justice Against Sponsors of Terrorism Act[5] (JASTA) "to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against [any person, entity, or foreign county that] provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States."[6] JASTA thus opened the door to new theories of liability against social media companies that assist a Foreign Terrorist Organization (FTO)[7] by explicitly including secondary liability and expanding the basis for tort claims.

---

[1] *See* Jytte Klausen, *The Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990-2015,* OFF. JUST. PROGRAMS (June 2016), https://www.ojp.gov/pdffiles1/nij/grants/250416.pdf [https://perma.cc/8SFY-AU8M]; Dep't Homeland Sec., *Strategic Framework for Countering Terrorism and Targeted Violence* 8 (2019); *Terrorist Groups Recruiting Through Social Media*, CBC NEWS (Jan. 10, 2012, 12:15 PM), https://www.cbc.ca/news/science/terrorist-groups-recruiting-through-social-media-1.1131053 [https://perma.cc/C5MX-5EW3] (quoting Professor Gabriel Weimann of the University of Haifa, who stated that "about 90 per cent of organized terrorism on the internet is being carried out through social media.").

[2] 18 U.S.C. § 2333 (2018).

[3] *See* Boim v. Holy Land Foundation for Relief and Development, 549 F.3d 685, 689 (7th Cir. 2008) (en banc).

[4] *Compare Boim*, 549 F.3d at 689 ("[S]tatutory silence on the subject of secondary liability means there is none.") *with* Wultz v. Islamic Republic of Iran, 755 F. Supp. 2d 1, 54–57 (D.D.C. 2010) ("[P]laintiffs may plead and have pled secondary liability [under the ATA].").

[5] Pub. L. No. 114-222, § 4(a), 130 Stat. 852, 854 (2016) (codified at 18 U.S.C. § 2333(d)).

[6] *Id.* at 853; *see also*, *e.g.*, Kaplan v. Lebanese Can. Bank SAL, 999 F.3d 842, 855 (2d Cir. 2021) (discussing the language).

[7] *See* 8 U.S.C. § 1189(a)(1).

Section 230 of the Communications Decency Act (CDA)[8] presents a significant hurdle to claims against social media companies. The CDA was implemented to protect children from explicit content online without penalizing interactive computer service providers for inadvertently allowing illegal content to slip through their filters.[9] To achieve this, the CDA has a "Good Samaritan" clause stating that service providers, such as social media companies, will not be treated as the publisher of content posted on their platform.[10] The effect is that service providers cannot be held liable for people's illegal use of their service unless those service providers took additional action or provided support to the users. Understanding the CDA and how it interacts with JASTA is critical to analyzing possible avenues for liability when an FTO's operations are assisted by social media.

The Supreme Court was set to clarify the application of CDA § 230 for social media involvement in acts of terrorism in *Gonzalez v. Google LLC*.[11] Instead, a different hurdle prevented that analysis: JASTA itself. In *Twitter, Inc. v. Taamneh*,[12] the Supreme Court found that the plaintiffs' claims[13] did not satisfy the "aids and abets, by knowingly providing substantial assistance" requirement of JASTA.[14] In her concurrence, Justice Jackson emphasized that *Twitter*'s holding is "narrow in important respects" and that "general principles of tort and criminal law . . . do not necessarily translate to other contexts."[15]

This Comment seeks to explore the gaps remaining after the 2023 *Twitter* opinion, to better understand how JASTA should be read in cases related to social media companies, and to consider the "other contexts" Justice Jackson alluded to in her concurrence. Part II of this Comment discusses how terrorist organizations use social media to recruit and conduct attacks. Part III looks at how aiding and abetting liability functions in other contexts, including JASTA claims when no social media is involved, the Alien Tort Claims Act, and the Security Exchange Act of 1934. Part IV considers how particular aspects of aiding and abetting liability discussed in the previous part apply to social media companies. Part V discusses issues related to social media and

---

[8] *See* 47 U.S.C. § 230(c)(1).

[9] Anna Elisabeth Jane Goodman, *When You Give a Terrorist a Twitter: Holding Social Media Companies Liable for Their Support of Terrorism*, 46 PEPP. L. REV. 147, 177–78 (2018).

[10] 47 U.S.C. § 230(c)(1).

[11] 598 U.S. 617 (2023) (per curiam).

[12] 598 U.S. 471 (2023).

[13] The analysis in *Twitter* applies to *Gonzalez* because "plaintiffs concede[] the allegations underlying their secondary-liability claims are materially identical to those at issue in *Twitter*." *Gonzalez*, 598 U.S. at 622.

[14] *See* 18 U.S.C. § 2333(d).

[15] *Twitter*, 598 U.S. at 507 (Jackson, J., concurring).

terrorism that secondary liability is not equipped to resolve. Part VI concludes the Comment by observing that because JASTA claims are unlikely to succeed against social media companies, alternative action needs to be taken to reduce FTO use of social media.

II. HOW TERRORIST ORGANIZATIONS USE SOCIAL MEDIA

To better contextualize the legal framework for aiding and abetting liability as applied to social media companies that assist FTO operations, it is important to first examine the role social media plays in FTO activities. FTOs do not hack or otherwise distort social media functions to achieve their ends; rather, "extremists largely use the same platforms for the same purposes as an average internet user."[16] While the benefits of social media to FTOs are "merely incidental" to social media companies' services and general business models,[17] terrorist groups use social media to expand their outreach to larger audiences much faster than they otherwise could.[18]

A major way FTOs use social media is to radicalize individuals to join their cause. In a framework explained by Professor Gabriel Weimann, the multistep process for online radicalization can be broken down into four phases: "'The Net,' 'The Funnel,' 'The Infection,' and 'The Activation.'"[19] Although this procedure for radicalizing susceptible individuals is possible without social media, social media tools provide assistance at every step of the process.

Under Weimann's framework, "The Net" consists of the FTO exposing a target audience to "a single undifferentiated pitch" with the expectation that some users will not interact with the pitch, but with the hope that others will.[20] Terrorist organizations can now cast a much larger "Net," as 61.4 percent of the global population uses social media—a percentage even greater among younger generations.[21] Social media also allows FTOs to play a more active role in reaching out to target audiences: "Social networking allows terrorists to reach out to their target audiences and virtually 'knock on their doors'—in contrast to older models of websites in which terrorists had to wait for visitors

---

[16] Alexandra T. Evans & Heather J. Williams, *How Extremism Operates Online: A Primer*, RAND CORP., Apr. 2022, at 7.

[17] *See Twitter*, 598 U.S. at 504.

[18] Paul Gill et al., *Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes*, 16 CRIMINOLOGY & PUB. POL'Y 99, 111 (2017).

[19] Gabriel Weimann, *Terrorist Migration to Social Media*, 16 GEO. J. INT'L AFF. 180, 183 (2015).

[20] *Id.*

[21] *Global Social Media Statistics*, DATAREPORTAL, https://datareportal.com/social-media-users [https://perma.cc/GEQ7-8BXD].

to come to them."[22] Recommendation algorithms further expand "The Net" by matching users who have viewed similar content to FTO messaging, helping FTOs reach their target audience in ways they themselves would otherwise be unable to coordinate.[23]

During "The Funnel," the FTO continues to interact with individuals who were receptive to the initial message through additional "exposure to religious, political, or ideological material."[24] The interactive nature of social media makes it easier for FTOs to maintain conversations with individuals in "The Funnel." Two-way communication creates small, diffused groups such that echo chambers, a phenomenon where individuals are exposed to similar messaging due to a positive feedback loop, and frequent messaging are possible with little awareness from the individual.[25] Radicalization takes time and persistence, and it is easier to connect to an individual with personalized, on-demand messaging as opposed to generalized, consistent communication.

Once the relationship is strong enough, the FTO proceeds to "The Infection," in which the individual is further exposed to stronger ideological material and encouraged to act on their beliefs, or "self-radicaliz[e]."[26] Finally, "The Activation" involves the FTO providing practical instructions on how to use explosives, weapons, poisons, and chemicals and potentially identifying targets for the individual to harm.[27] Individuals who pass through all four stages have the potential to cause mass harm through an attack.

While FTOs have nefarious plans in mind, their use of social media boils down to sharing ideas and information—just as it does for a regular user. Bad actors using communication services for illicit ends is not new. The Supreme Court notes it generally will not find that "internet or cell service providers incur culpability merely for providing their services to the public writ large."[28] This boundary is necessary to prevent any service that provides social utility, such as cell phones, email, or the general internet, from being found liable for providing access to bad actors.[29] But it is also critical to acknowledge that social media assists terrorist organization operations exponentially more than phones, mail, or basic internet forums. When evaluating aiding and abetting liability, two ideas to keep in mind are how social media differs from traditional

---

[22] Weimann, *supra* note 19, at 182.

[23] *See* Joe Whittaker et al., *Recommender Systems and the Amplification of Extremist Content*, 10 INTERNET POL'Y REV. 1, 6–7 (2021).

[24] Weimann, *supra* note 19, at 184.

[25] *See* Walter Quattrociocchi, *Inside the Echo Chamber*, 315 SCI. AM. 4, 62–63 (2017).

[26] *See* Weimann, *supra* note 19, at 184.

[27] *Id.*

[28] Twitter v. Taamneh, 598 U.S. 471, 499 (2023).

[29] *See id.* at 500.

communication and if there are additional legal responsibilities for social media companies because of those differences.

III. LEGAL BACKGROUND

A. Analysis in *Twitter*

The plaintiffs' case in *Twitter* stemmed from the 2017 terrorist attack on the Reina nightclub in Istanbul, Turkey conducted by the Islamic State of Iraq and Syria (ISIS).[30] The plaintiffs claimed that defendant social media companies Facebook, Google (which owns YouTube), and Twitter had known for years that ISIS was using their platforms, profited from their content through third-party advertisers, and expanded their content's reach through recommendation algorithms.[31] The plaintiffs then argued this was sufficient to hold that the social media companies aided and abetted ISIS by "knowingly providing substantial assistance" under § 2333(d)(2).[32] The Ninth Circuit found that plaintiffs had plausibly alleged that the defendant social media companies aided and abetted ISIS within the meaning of § 2333(d)(2).[33] The Supreme Court disagreed and dismissed for failure to state a claim after addressing two questions: "First, what exactly does it mean to 'aid and abet'? Second, what precisely must the defendant have 'aided and abetted'?"[34]

1. The meaning of "aid and abet": *Halberstam v. Welch*[35]

The phrase "aid and abet" is not defined in JASTA. Instead, Congress points to *Halberstam*[36] to "provid[e] the proper legal framework" for "civil aiding-and-abetting and conspiracy liability."[37] In *Halberstam*, the D.C. Circuit analyzed "a series of state and federal cases, the Restatement (Second) of Torts, and prominent treatises that discussed secondary liability in tort."[38] *Halberstam* identifies three main elements of aiding and abetting. First, "the party whom the defendant aids must perform a wrongful act that causes an injury."[39] Second, "the defendant must be generally aware of his role as part of an overall illegal or

---

[30] *See id.* at 478.

[31] *Id.* at 480–82.

[32] *Id.* at 481–82.

[33] Gonzalez v. Google LLC, 2 F.4th 871 at 880 (9th Cir. 2021).

[34] *Twitter*, 598 U.S. at 484 (internal quotations omitted).

[35] 705 F.2d 472 (D.C. Cir. 1983).

[36] *See infra* Part III.B for background and discussion of *Halberstam*.

[37] *Twitter*, 598 U.S. at 485 (citing § 2(a)(5), 130 Stat. 852).

[38] *Id.* at 486; *Halberstam*, 705 F.2d at 476–478, 481–486.

[39] *Halberstam*, 705 F.2d at 477.

tortious activity at the time that he provides the assistance."[40] Third, "the defendant must knowingly and substantially assist the principal violation."[41] *Halberstam* notes that those who aid and abet a tortious act may be liable not only for the act itself, but also for other reasonably foreseeable acts in connection with the primary tort.[42]

The Court in *Twitter* determined that the first two elements were satisfied: ISIS caused an injury through the attacks and the companies were generally aware that ISIS was using their platforms. With the first two elements not in dispute, the Court's analysis focused on the third element, "knowingly and substantially assisting the principal violation." At the outset, the Court noted that "the concept of 'helping' in the commission of a crime—or a tort—has never been boundless."[43] Specifically, the tort system does not tend to impose liability for inactions or nonfeasance; some level of blameworthiness is required. Courts need to confine aiding and abetting liability to "truly culpable conduct," as the liability "does not require any agreement with the primary wrongdoer to commit wrongful acts, thus eliminating a significant limiting principle."[44]

The "knowing" half of "knowing and substantial assistance" is "designed to capture the defendants' state of mind with respect to their actions and the tortious conduct."[45] In determining if assistance was "substantial," *Halberstam* articulates six factors: "(1) the nature of the act encouraged, (2) the amount of assistance given by defendant, (3) defendant's presence or absence at the time of the tort, (4) defendant's relation to the principal, (5) defendant's state of mind, and (6) the period of defendant's assistance."[46] *Halberstam* cautions that these factors should not be viewed as immutable components, but instead be "adapted as new cases test their usefulness in evaluating vicarious liability."[47]

The Court clarified that the "knowing" and "substantial" requirements work "in tandem, with a lesser showing of one demanding a greater showing of the other."[48] That is to say, "less substantial assistance require[s] more scienter before a court [can] infer conscious and culpable assistance. And, vice versa, if the assistance were direct and

---

[40] *Id.*

[41] *Id.*

[42] *See id.* at 484.

[43] *Twitter*, 598 U.S. at 488.

[44] *Id.* at 489–90.

[45] *Id.* at 504.

[46] Gonzalez v. Google LLC, 2 F.4th 871, 904 (9th Cir. 2021) (citing *Halberstam*, 705 F.2d at 483–84).

[47] *Halberstam*, 705 F.2d at 489.

[48] *Twitter*, 598 U.S. at 491–492.

extraordinary, then a court might more readily infer conscious participation in the underlying tort."[49] When applying this sliding-scale approach, it is important for courts not to confuse the "knowing" half of "knowing and substantial assistance" with the general knowledge requirement.[50] A general awareness that terrorist activities are occurring and a specific knowledge of assisting those activities are different inquiries.

2. What defendants must have "aided and abetted"

The language of JASTA does not specify exactly what must be aided and abetted. In *Twitter*, the plaintiffs asserted that "the person" conducting acts of terrorism must be aided and abetted such that generally aiding and abetting ISIS members would be sufficient.[51] Under this theory, assisting the eventual perpetrator of an attack would be enough for liability. Defendants insisted it is instead "the act of international terrorism" that must be aided and abetted, requiring a "strict nexus" between the assistance and the Reina nightclub attack.[52]

The Supreme Court held that both arguments were too narrow.[53] It is not sufficient that a defendant provides "substantial assistance to a transcendent 'enterprise' separate from and floating above all the actionable wrongs that constitute it."[54] On the other hand, it is not necessary for "the defendant to have known all particulars of the primary actor's plan."[55] The Court did not set clear lines, stating that "a close nexus between the assistance and the tort might help establish that the defendant aided and abetted the tort, but even more remote support can still constitute aiding and abetting *in the right case*."[56]

3. Limitations by the facts of *Twitter*

The analysis in *Twitter* is helpful for understanding the aiding and abetting requirement of § 2333(d)(2), but the facts of the case severely limit its utility. The plaintiffs in *Twitter* did not allege that the perpetrator of the Reina attacks was recruited through social media, used social media to plan the attack, or even used social media at all.

---

[49] *Id.* at 492.

[50] *See* Nathan I. Combs, Note, *Civil Aiding and Abetting Liability*, 58 VAND. L. REV. 241, 267–278 (2005) (describing the history of the sliding-scale approach and arguing against it).

[51] *Twitter*, 598 U.S. at 494.

[52] *Id.*

[53] *See id.*

[54] *Id.* at 495.

[55] *Id.* (internal quotations omitted).

[56] *Id.* at 496 (emphasis added).

Rather, the plaintiffs alleged that the social media companies used recommendation algorithms to match ISIS-related content with users.[57] While it may have extended the reach of ISIS, the Court did not find that the recommendation algorithms constituted "active, substantial assistance."[58] In line with the sliding-scale approach, the Court held that providing services available to the public is not enough; instead, acts along the lines of "special treatment or words of encouragement"[59] are necessary to show assistance.

The Court also did not entertain the plaintiffs' allegation that the social media companies "took insufficient steps to ensure that ISIS supporters and ISIS-related content were removed from their platforms."[60] An argument that relies so heavily on inaction "might have more purchase if [the plaintiffs] could identify some independent duty in tort that would have required defendants to remove ISIS' content," but the plaintiffs did not allege such a duty in their complaint.[61] Even if such a duty was identified, the "distant inaction" between the social media companies and ISIS could not have led to knowing and substantial assistance.[62] The Court did note that "there may be situations where some such duty exists," but that question was not addressed in *Twitter*.[63]

Lastly, an allegation specific to Google involved revenue sharing. The plaintiffs alleged that Google approved ISIS videos uploaded to YouTube for monetization, placed advertisements in proximity to the videos, shared revenue from those advertisements with ISIS and ISIS-affiliated users, and failed to remove the videos after they were reported.[64] The Supreme Court agreed with the Ninth Circuit's reasoning and found the allegation failed to state a claim because it did not allege how much assistance Google provided, meaning such assistance could not be "substantial."[65]

The Court held that the actions of the social media companies in *Twitter* were simply far too attenuated from the Reina nightclub attack to draw any inference of knowing, substantial support under § 2333(d)(2).[66] As a result, it remains unclear how much support is considered enough in other contexts.

---

[57] *Id.* at 498.

[58] *Id.* at 499.

[59] *Id.* at 498.

[60] *Id.*

[61] *Id.* at 501.

[62] *Id.*

[63] *Id.*

[64] Gonzalez v. Google LLC, 2 F.4th 871, 881–882 (9th Cir. 2021).

[65] *Twitter*, 598 U.S. at 505.

[66] *Id.* at 500, 506–07.

B. *Halberstam* in Other Contexts

In enacting JASTA, Congress "took the unusual step of specifying a decision,"[67] *Halberstam*, to provide the "proper legal framework"[68] for aiding and abetting liability. The details of this case make it difficult to apply to situations involving social media companies.

Halberstam addressed whether the defendant, Linda Hamilton, was liable for aiding and abetting the killing of Michael Halberstam by Bernard Welch, Hamilton's long-term business colleague and romantic partner.[69] Welch and Hamilton lived together, and Welch would leave the house most evenings for approximately four hours.[70] Unbeknownst to Hamilton, Welch used this time to burglarize houses, creating a supply for his coin "business."[71] Hamilton helped Welch operate this business through bookkeeping, depositing buyers' checks in her name, and falsifying tax records—all while remaining unaware of Welch's burglaries.[72] Hamilton and Welch rapidly accumulated significant wealth from this venture.[73] Eventually, one of Welch's burglaries went bad, resulting in Welch shooting and killing Halberstam.[74] Hamilton was not present during the killing, nor was she aware it even occurred.[75] But the D.C. Circuit found Hamilton guilty for aiding and abetting the murder because she was "generally aware of her role in Welch's criminal enterprise" and "had given knowing and substantial assistance to Welch's activities."[76]

"The scenario presented in *Halberstam* is, to put it mildly, dissimilar"[77] to social media companies providing assistance to terrorist organizations. Given the unique congressional directive to use the *Halberstam* framework and the imprecision of the knowing and substantial assistance standard, this Comment explores how the standard has previously been applied to large corporations to provide insight as to how *Halberstam*'s holding might apply to social media companies.

---

[67] Freeman v. HSBC Holdings, 57 F.4th 66, 76 (2d. Cir. 2023).

[68] Pub. L. No. 114-222 § 2(a)(5), 130 Stat. at 852 (2016).

[69] *See* Halberstam v. Welch, 705 F.2d 472, 474 (D.C. Cir. 1983).

[70] *See id.* at 475.

[71] *Id.*

[72] *See id.*

[73] *See id.*

[74] *See id.*

[75] *See id.*

[76] Twitter v. Taamneh, 598 U.S. 471, 487 (2023).

[77] Gonzalez v. Google LLC, 2 F.4th 871, 902 (9th Cir. 2021).

1. Participation in a Scheme

In *Atchley v. AstraZeneca*,[78] victims of numerous attacks by Jaysh al-Mahdi,[79] an Iraqi militia, brought a claim against multiple large medical supplies companies. From 2000–2003, the United Nations established an "Oil-for-Food" program that allowed Iraq to bypass sanctions and sell oil "for the limited purpose of purchasing essential food and medical supplies for its people."[80] The goods went through Kimadia, Iraq's state-owned import company operated by the Ministry of Health.[81] Jaysh al-Mahdi used the Ministry of Health and Kimadia as a front for its terrorist activities.[82] Kimadia exploited the humanitarian program, "circumventing the program's limits by extracting a 10% cash kickback from humanitarian-goods suppliers. And Kimadia required suppliers to provide free medical goods—typically 10% in excess of the underlying contract quantities."[83] These kickbacks and extra medical supplies were used to fund Jaysh al-Mahdi's operations.[84] Multiple news articles made this arrangement known, yet the medical companies continued to supply Kimadia.[85]

To determine if the medical companies' actions constituted knowing and substantial assistance, the court walked through the six *Halberstam* factors. For the nature of the act assisted, the court noted that "[f]inancial support is 'indisputably important' to the operation of a terrorist organization, and any money provided to the organization may aid its unlawful goals."[86] Therefore, the medical supply companies assisted the act of "violent terrorizing, maiming, and killing of U.S. nationals in Iraq" through their monetary assistance to Jaysh al-Mahdi.[87] For the amount and kind of assistance, the complaint alleged "that defendants gave Jaysh al-Mahdi at least several million dollars per year in cash or goods over a period of years."[88] The court rejected the argument that the monetary assistance needed to be "indispensable to the injurious acts for this factor to weigh in support of liability."[89] For the

---

[78] 22 F.4th 204 (D.C. Cir. 2022).

[79] Although Jaysh al-Mahdi was not a designated FTO, the court found that Hezbollah, an FTO, committed, planned, or authorized the attacks. *Id.* at 216–219.

[80] *Id.* at 211.

[81] *Id.* at 210–11.

[82] *Id.* at 212.

[83] *Id.* at 211.

[84] *See id.* at 209.

[85] *See id.* at 213.

[86] *Id.* at 222 (citing Gonzalez v. Google LLC, 2 F.4th 871, 905 (9th Cir. 2021)).

[87] *Id.*

[88] *Id.*

[89] *Id.*

state of mind factor, the court held that "[k]nowledge of one's own actions and general awareness of their foreseeable results, not specific intent, are all that is required."[90] This went against the district court's ruling that required the defendant's state of mind to be the same as Jaysh al-Mahdi's: a "desire to kill American citizens in Iraq or . . . to help [Jaysh al-Mahdi] succeed in doing so."[91] Lastly, the court found that four years was a significant amount of time for the duration factor.[92]

A key point of differentiation between *Atchley* and *Twitter* is that the *Atchley* defendants voluntarily participated in the scheme. Social media companies may have general awareness that terrorist organizations use their platforms, but it is not plausible to allege that they voluntarily participate in a scheme with FTOs; social media companies do not want FTOs on their platform and consistently attempt to remove them.[93]

2. Routine Services

The Second Circuit considered how JASTA applies to banks in *Siegel v. HSBC North America Holdings*.[94] The defendant bank, HSBC, "maintained a commercial relationship with Al Rajhi Bank ('ARB'), Saudi Arabia's largest bank, with approximately $80 billion in assets and more than 500 branches worldwide."[95] HSBC provided ARB with a wide range of banking services despite knowing that ARB had ties to al-Qaeda, an FTO.[96] HSBC was also involved in a scheme that allowed ARB to transfer hundreds of millions of dollars in ways designed to "circumvent monitoring by U.S. regulators."[97] After twenty-five years of this arrangement, al-Qaeda suicide bombers conducted a series of coordinated attacks (the November 9 Attacks).[98] Families of the victims sued HSBC for violating JASTA by aiding and abetting al-Qaeda's attacks.

The Second Circuit held that, despite HSBC's knowledge of ARB's ties to al-Qaeda and its scheme to evade U.S. regulation, plaintiffs had

---

[90] *Id.* at 223.

[91] Atchley v. AstraZeneca, 474 F.Supp.3d 194, 213 (D.D.C. 2020); *see also* Bernhardt v. Islamic Republic of Iran, 47 F.4th 856, 872 (D.C. Cir. 2022) (holding that there is no "one in spirit" requirement for the state of mind factor).

[92] *Atchley*, 22 F.4th at 224.

[93] *See infra* Part IV.D.

[94] 933 F.3d 217 (2d. Cir. 2019).

[95] *Id.* at 220.

[96] *Id.*

[97] *Id.* at 221.

[98] *See id.* at 219.

not properly alleged that HSBC was aware it was "playing a role" in al-Qaeda activities.[99] HSBC provided "routine banking services to a foreign, unaffiliated financial institution" and plaintiffs failed "to advance any plausible, factual, non-conclusory allegations that HSBC knew or intended that those funds would be sent to [al-Qaeda] or to any other terrorist organizations."[100] Further, HSBC cut off ties with ARB ten months prior to the November 9 Attacks because it had concerns about financing terrorism.[101] Cutting off the relationship convinced the court that HSBC could not have "knowingly assumed a role in the [November 9] Attacks."[102]

Only providing routine services is not an all-encompassing safeguard, however, as shown in *King v. Habib Bank Limited*.[103] As in *Siegel*, the plaintiffs in *King* were victims of terrorist attacks conducted by al-Qaeda and brought action against the defendant bank, Habib Bank Limited, that had ties to ARB.[104] Here, the defendant Habib Bank Limited had abused regulatory requirements by placing known terrorists or terrorist affiliates on "whitelists," giving those parties pre-clearance for reduced scrutiny of their transactions.[105] The New York Department of Financial Services (NYDFS) investigated the bank's practices in 2006, and the bank agreed to heighten its anti-money laundering procedures.[106] In 2015, the bank again committed to reform its standards after failing to do so initially.[107] Two years later, the NYDFS charged the bank with several violations "due to ongoing deficiencies including . . . Defendant's diligence on ARB, its 'whitelist,' and its concealment of suspicious transactions."[108]

The defendants in *King* relied on *Siegel* as precedent that providing routine services to a bank "which may have later made funds available to FTOs through several intermediaries" did not amount to substantial assistance.[109] The court differentiated the claims from those in *Siegel*, stating, "HSBC ended the relationship after learning of ARB's ties to terrorism, while Defendant here is alleged to have doubled down."[110] Thus, the court held that providing routine services can still be cause

---

[99] *Id.* at 224.

[100] *Id.* at 223–25.

[101] *Id.* at 221.

[102] *Id.* at 224.

[103] No. 20-CV-4322, 2022 WL 4537849 (S.D.N.Y. Sept. 28, 2022).

[104] *See id.* at *1.

[105] *See id.*

[106] *See id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* at *9.

[110] *Id.*

for liability when coupled with additional misconduct that indicates the defendant's intent.[111]

The combination of providing routine services with questionable conduct by the defendant was further considered in *Bonacasa v. Standard Chartered PLC*,[112] which was reconsidered in light of *Twitter*. Standard Chartered Bank provided banking services to the Fatima Group, "a Pakistani fertilizer company that purportedly supplied Al-Qaeda with materials used to make improvised explosive devices ('IEDs')."[113] The U.S. government contacted the Fatima Group to attempt to work together to control the distribution of the main explosive material, calcium ammonium nitrate (CAN).[114] Once working directly with the Fatima Group proved unsuccessful, the U.S. government contacted Standard Chartered with evidence that the Fatima Group was supplying materials responsible for "80% of the IEDs used against American service members in Afghanistan" and asked them to end the business relationship with the Fatima Group.[115] Standard Chartered instead "continued to provide substantial project financing to Fatima" including a "'specially structured' loan specifically for the purpose of removing CAN production bottlenecks and increasing Fatima's CAN production capacity."[116]

The *Bonacasa* court found that plaintiffs successfully alleged that Standard Chartered aided and abetted terrorism under JASTA, noting "the gravamen of Plaintiffs' claims is not that Standard Chartered simply failed to discontinue its prior ongoing financial or banking services to Fatima after the January 2013 meeting, but that it thereafter affirmatively funded Fatima with the specific intent of removing barriers to CAN production."[117] In reconsideration, the opinion notes that "*Twitter* directs courts to focus on the *defendant's actions* vis-à-vis the specific attack that injured the plaintiffs, rather than the *terrorist enterprise's actions* vis-à-vis defendant's services or how valuable defendant's services were to the enterprise."[118] The court reiterated that JASTA does not require a strict nexus such that the knowing and substantial assistance requirement "can be satisfied even where the defendant did not intentionally aid the specific terrorist *attack* itself."[119]

---

[111] *Id.* at *10.

[112] No. 22-CV-3320, 2023 WL 7110774 (S.D.N.Y. Oct. 27, 2023).

[113] *Id.* at *1.

[114] *Id.* at *2.

[115] *Id.* at *3.

[116] *Id.*

[117] *Id.* at *10.

[118] *Id.* at *9 (emphasis in original).

[119] *Id.* (emphasis in original).

Providing routine banking services with clear knowledge of how those services are used is sufficient for aiding and abetting liability.

As alluded to in *Twitter*, providing routine services "in an unusual way" "could constitute aiding and abetting a foreseeable terror attack."[120] *Zobay v. MTN Group Limited*[121] considered JASTA claims against two telecommunication companies. The first, MTN Group, allegedly entered a joint venture with the Iran Electronic Development Company (IEDC), a known front for an FTO, the Islamic Revolutionary Guard Corps (IRGC).[122] The court found that plaintiffs properly alleged that MTN aided and abetted IRGC under § 2333(d)(2) because MTN's partnership with IRGC constituted "a relationship that is both far less passive and far less attenuated than what plaintiffs were able to allege in [*Twitter*]."[123] Specifically, when MTN entered the joint venture, its CEO signed an agreement letter that was "'replete with indicia' that it was drafted by the IRGC" and hid the fact that the agreement existed, using a codename in internal documents.[124] MTN also evaded U.S. sanctions to procure their technologies to the IEDC and allowed Iranian military intelligence officials to occupy the second floor of their Iran offices.[125] The court found that the unusual business arrangements made it foreseeable that "goods and funds would flow to proxy groups and that acts of terror would result."[126] Additionally, the services MTN provided to the IEDC were not generally available to the public, "so the IRGC's ability to benefit was not 'merely incidental' to the availability of a preexisting platform."[127] While the court distinguished the public availability aspect, it also noted that the "Second Circuit has emphasized that facially neutral acts (such as providing communications services) must be assessed in the context of the enterprise they aided—that is, against the historical background of the FTO's activities."[128]

Huawei U.S., the second telecommunications company in *Zobay*, allegedly contracted with three IRGC fronts to acquire embargoed U.S. technologies for their Iranian business partners.[129] According to the court, the plaintiffs did not properly allege aiding and abetting for Huawei because the complaint failed to allege an amount of assistance

---

[120] Twitter v. Taamneh, 598 U.S. 471, 502 (2023).

[121] 695 F. Supp. 3d 301 (E.D.N.Y. 2023).

[122] *See id.* at 318.

[123] *Id.* at 347.

[124] *Id.* at 318.

[125] *See id.* at 346.

[126] *Id.*

[127] *Id.* at 349.

[128] *Id.* at 337 (citing Kaplan v. Lebanese Can. Bank SAL, 999 F.3d 842, 865 (2d Cir. 2021)) (internal quotations omitted).

[129] *Id.* at 351–52.

that would indicate Huawei "culpably associated itself with the terrorist group's actions."[130] Huawei's conduct was focused on evading government interference, meaning "plaintiffs would need some other very good reason to think that defendants were consciously trying to help or otherwise participate in" the terrorist attacks.[131] Although both MTN and Huawei operated by violating U.S. sanctions, the details of their business arrangements mattered in determining their purpose and consequent culpability.

C. Non-*Halberstam* Cases

Although Congress pointed to *Halberstam* for the proper theory of civil aiding and abetting liability, the Court noted that they "generally presume that such common-law terms 'brin[g] the old soil' with them."[132] Therefore, cases that analyze if large corporations are liable for aiding and abetting may also be illuminating. Statutory civil aiding and abetting liability is not particularly common, and much ink has been spilled in determining if secondary liability claims are permissible, just like for the ATA before JASTA.[133] The following section focuses on decisions rendered when courts still operated under the ruling that plaintiffs could pursue civil aiding and abetting claims.

1. The Alien Tort Claims Act (ATCA)[134]

The Supreme Court has articulated "the standard for imposing accessorial liability under the [ATCA] must be drawn from international law."[135] Aiding and abetting liability under the ATCA imposes a higher standard than that outlined in *Halberstam*; a claimant must show the defendant not only provided substantial assistance but also had the purpose of facilitating the act of terrorism.[136]

Providing particular convenience to bad actors is not sufficient for aiding and abetting liability under the ATCA. In *Presbyterian Church of Sudan v. Talisman Energy*, a Canadian oil company, Talisman

---

[130] *Id.* at 353.

[131] *Id.* at 354 (internal quotations omitted).

[132] Twitter v. Taamneh, 598 U.S. 471, 484 (2023).

[133] *See, e.g.*, Andrei Takhteyev, Note, *Who Is to Blame? (and What Is to Be Done?): Liability of Secondary Actors Under Federal Securities Laws and the Alien Tort Claims Act*, 74 BROOK. L. REV. 1539, 1540 (2009).

[134] The Alien Tort Claim Act has many jurisdictional concerns, *see* Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108 (2013), but this section focuses only on the aiding and abetting analysis under the statute.

[135] Presbyterian Church of Sudan v. Talisman Energy, 582 F.3d 244, 247 (2d. Cir. 2009) (citing Sosa v. Alvarez–Machain, 542 U.S. 692 (2004)).

[136] *Id.*

Energy, undertook an oil extraction endeavor in Sudan amidst the Second Sudanese Civil War.[137] Due to securities concerns involving the war, the oil company worked with the Sudanese government to build roads that connected different oil extraction sites.[138] The roads "served the dual purposes of moving personnel for oil operations and facilitating military activities."[139] The roads assisted the ability of the Sudanese government to injure and displace residents of southern Sudan. The victims sued the oil company for aiding and abetting those injuries.[140] The Second Circuit held that the oil company was not liable for aiding and abetting the actions of the Sudanese government because the oil company did not act with the purpose of assisting the government's human rights violations; their purpose was to improve their oil operations.[141]

In contrast, benefitting from the underlying tort is sufficient for aiding and abetting under the ATCA. In *Doe I v. Nestle USA, Inc.*,[142] three former child slaves in the Ivory Coast sued Nestle and other companies for aiding and abetting child slavery by providing assistance to Ivorian farmers.[143] At the time, the Ivory Coast produced 70 percent of the world's cocoa supply.[144] Despite the well-known practice of using child labor for the cocoa farming operations, the defendants offered financial and technical farming assistance to maintain relationships with the local farmers.[145] The Ninth Circuit found that "the defendants have not merely profited by doing business with known human rights violators. Instead, they have allegedly sought to accomplish their own goals by supporting violations of international law."[146] Because the defendants directly benefitted from the child slavery through reducing costs, the court found that their support to farmers satisfied the mens rea for aiding and abetting child slavery, which is analogous to the "knowing" portion of knowing and substantial assistance.[147] These two cases differentiate between situations in which a company takes a legitimate business action that incidentally provides a particular convenience to tortfeasors and ones which the alleged aider and abettor takes action to

---

[137] *See id.* at 248–49.

[138] *See id.* at 249.

[139] *Id.*

[140] *Id.* at 247.

[141] *See id.* at 259.

[142] 766 F.3d 1013 (9th Cir. 2014).

[143] *See id.* at 1016.

[144] *Id.* at 1017.

[145] *See id.*

[146] *Id.* at 1024.

[147] *Id.* at 1026.

perpetuate the tort and continue to directly benefit from principal violation.

2. The Securities Exchange Act of 1934[148]

Section 10(b) of the Securities Exchange Act of 1934 ("the Exchange Act") makes it "unlawful for any person" to "directly or indirectly" "employ . . . any manipulative or deceptive device or contrivance" in "connection with the purchase or sale of any security."[149] Section 10(b) itself does not contain an explicit basis for aiding and abetting liability, only primary liability.[150] Courts first held that a right of action for aiding and abetting federal securities law existed in *Brennan v. Midwestern United Life Insurance Company*.[151] Due to the frequency of fiduciary duties or duties to disclose in securities law, there is much discussion about how recklessness impacts the knowledge aspect of aiding and abetting.

Through Exchange Act cases, there is precedent for courts to find recklessness in aiding and abetting claims even when it is not explicitly mentioned in the statute. As it currently reads, the Exchange Act states that "any person that knowingly or recklessly provides substantial assistance to another person in violation of a provision of this chapter" may be liable for aiding and abetting the violations.[152] The term "recklessly" was added to the Exchange Act by the Dodd-Frank Act of 2010 amendments,[153] but courts found "[s]evere recklessness can satisfy the scienter requirement in an aiding and abetting case, at least where the alleged aider and abettor owes a duty to the defrauded party"[154] in cases litigated before "recklessly" appeared in the statutory text of the Dodd-Frank Act. Parties argued that "Congress's amendment to include recklessness remove[s] all doubt that, prior to the Dodd–Frank Act, actual knowledge was required."[155] In *Big Apple Consulting*, the Eleventh Circuit looked to legislative history to confirm that the amendment was meant to reinforce the use of the recklessness standard.[156]

---

[148] Pub. L. No. 73–291, 48 Stat. 881 (codified at 15 U.S.C. § 78a).

[149] 15 U.S.C. § 78j(b).

[150] *See* Alan R. Bromberg & Lewis D. Lowenfels, *Aiding and Abetting Securities Fraud: A Critical Examination*, 52 ALB. L. REV. 637, 643–46 (1988).

[151] 286 F. Supp. 702 (N.D. Ind. 1968).

[152] 15 U.S.C. § 78t(e).

[153] *See* SEC v. Big Apple Consulting USA, 783 F.3d 786, 800 (11th Cir. 2015).

[154] Woods v. Barnett Bank of Ft. Lauderdale, 765 F.2d 1004, 1010 (11th Cir. 1985).

[155] *Big Apple Consulting*, 783 F.3d at 800–801 (internal quotations omitted).

[156] *See id.* at 799–801.

IV. APPLYING CIVIL AIDING AND ABETTING THEORY TO SOCIAL MEDIA

A. Does "Recklessness" Matter for Social Media?

As noted previously, Congress intended JASTA "to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against [any person or entity that] provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States."[157] In line with providing the broadest possible basis, Congress also noted in its findings that "[p]ersons, entities, or countries that knowingly *or recklessly* contribute material support or resources, directly or indirectly, to persons or organizations that pose a significant risk of committing acts of terrorism . . . should reasonably anticipate being brought to court in the United States to answer for such activities."[158] From this, it appears that if social media companies are reckless in allowing bad actors to use their platforms for nefarious purposes, it may open the door to liability.

One case has already considered recklessness as it relates to "knowing and substantial assistance" for social media companies aiding and abetting terrorism. In *Cain v. Twitter*,[159] family members of individuals killed in large-scale terrorist attacks conducted by ISIS sued Twitter because it "knew about [the terrorist] activity but made minimal and largely ineffective efforts to curtail it."[160] The court found that pleading Twitter's knowledge of an FTO's usage of the platform amounted to an allegation of recklessness, but that JASTA required more.[161] The court reasoned that although "Congress referred in its statement of findings and purpose to those who 'knowingly *or recklessly* contribute material support or resources' to terrorists . . . the plain language of Section 2333 reaches only those 'knowingly providing substantial assistance.' This clear statutory text controls."[162] Because the mention of recklessness only appears in the legislative history, the court thought it insufficient to use that standard.

As mentioned above, courts have found recklessness as a relevant consideration for aiding and abetting liability without explicit statutory direction in the Exchange Act.[163] JASTA considers the elements of

---

[157] Pub. L. No. 114-222, § 2(b), 130 Stat. 853 (2016).

[158] *Id.* at § 2(a)(6) (emphasis added).

[159] No. 17-CV-02506-JD, 2018 WL 4657275 (N.D. Cal. Sept. 24, 2018).

[160] *Id.* at *1.

[161] *See id.* at *3.

[162] *Id.*

[163] *See supra* Part III.D.2.

Halberstam "in light of the common law."[164] Legislative history may be sufficient to impose a recklessness standard despite not being present in the statutory text. A glaring difference between the Exchange Act and JASTA is that for securities cases, a duty is owed to the defrauded party; no such duty was plead in *Twitter*. As *Twitter* notes, "inaction cannot create liability as an aider and abettor absent a duty to act."[165] It is the absence of this duty, not omission from the text, that removes the recklessness standard from the equation.

Gonzalez v. Google LLC includes an argument advanced by plaintiffs regarding an independent duty to act as it relates to § 2339B(a)(1), which criminalizes "providing material support or resources to designated foreign terrorist organizations."[166] The Ninth Circuit cautioned that because the general knowledge requirement for JASTA involves only awareness of the organization's connection to terrorism and not intent to further the tortious activities, "the *mens rea* required for the general awareness element of secondary liability under § 2333(d) may not be coextensive with the showing required for material support under § 2339B."[167] Thus, the court did not find an independent duty to not provide material support to terrorist organizations.

B. "Routine Services" for Social Media

If alleged aiders and abettors provide routine services in an unusual way, courts are more likely to find they provided knowing and substantial assistance.[168] But what constitutes routine services? Must those services be available to everyone who uses the platform, or only accessible to most users? In attempting to answer those questions, the Supreme Court in *Twitter* pointed to a case of a registered morphine distributor mailing excessive amounts of the drug,[169] but that case does not provide sufficient guidance for social media cases.

Classifying "routine services" compared to the baseline user of the platform may miss the mark. A straightforward example is a service in which users can pay the platform to artificially boost their content in the platform's recommendation algorithm. This service is available to all willing users, but it is not "routine" in the sense that a typical user does not utilize the service. Defining "routine services" in the context of other social media companies does not quite work either. Every social

---

[164] Twitter v. Taamneh, 598 U.S. 471, 497 (2023).

[165] *Id.* at 491 (internal quotations omitted).

[166] 18 U.S.C. § 2339B(a)(1).

[167] Gonzalez v. Google LLC, 2 F.4th 871, 903 (9th Cir. 2021).

[168] *See supra* Part III.B.2.

[169] *See Twitter*, 598 U.S. at 502 (summarizing Direct Sales Co. v. United States, 319 U.S. 703 (1943)).

media company is attempting to differentiate themselves, so they are incentivized to create new and unique features for their platform. Suppose a social media company creates a successful, often-used virtual reality space, and that space facilitates FTO activities by allowing terrorists to physically train individuals on how to conduct attacks in real time. It would be a stretch to claim the social media company is providing routine services in an unusual way that makes them more culpable for aiding and abetting terrorism.

As social media companies expand in reach and develop new services, the definition of routine services will become more pressing. Likely, it will be a moving target that is difficult to pinpoint. If the services are always viewed in the context of direct support to terrorist activities, then the utility of social media companies to terrorist groups might significantly increase so long as the services also have utility for other users.

C. Revenue Sharing Through Social Media

As noted in *Gonzalez*, "[f]inancial support is 'indisputably important' to the operation of a terrorist organization, and any money provided to the organization may aid its unlawful goals."[170] Social media companies may share revenue with terrorist organizations from advertisements placed near the FTO's content. There are relatively few cases that consider how revenue sharing impacts a JASTA claim. In *Gonzalez*, the revenue sharing claim failed because the complaint was "devoid of any allegations about how much assistance Google provided."[171]

Another issue exists in how exactly users join the revenue sharing systems. The *Gonzalez* plaintiffs alleged that "Google reviewed and approved ISIS videos for monetization."[172] Does this mean that the terrorist organization opted into the revenue sharing system and an automated system approved the request, or that an individual parsed through every video posted by the terrorist organization and then gave the approval? The difference may have important consequences as the latter situation allows for a stronger argument that the social media company provided "knowing" assistance.[173]

Claims that involve revenue sharing are stronger than claims without because revenue sharing weighs more heavily on the "substantial" side of the "knowing and substantial assistance" sliding-scale. Exactly

---

[170] *Gonzalez*, 2 F.4th at 905 (citing Halberstam v. Welch, 705 F.2d 472, 488 (D.C. Cir. 1983)).

[171] *Id.* at 907.

[172] *Id.* at 905.

[173] *See infra* Part V.

how much money needs to be shared would be fact-specific based on the other circumstances surrounding the claim.

D. Elements of a (Potentially) Successful Claim

With everything discussed in mind, future plaintiffs will have difficulty bringing a successful JASTA claim against social media companies. To showcase this difficulty, consider the elements of a JASTA claim against a social media company that has the best chance of withstanding a motion to dismiss. This Comment assumes that the claim does not include any direct contact with the FTO and that the social media company provided routine services in usual ways. Both stipulations would make the claim much stronger, but it is unrealistic that a major social media company would do either.

First, the FTO receives or will receive revenue sharing from the social media platform. Again, this bolsters the claim because courts have emphasized how important financial support is to the illegal activities of FTOs.[174] Second, the plaintiffs allege a specific amount of monetary assistance provided to the FTO. Alleging a specific amount is possible by using estimates of how much platforms give through revenue sharing and the number of views on FTO videos to approximate the total amount of financial assistance.[175] A larger amount increases the viability of the claim, but alleging a specific number at least gives the court the opportunity to find the amount to be "substantial."

Third, the FTO has operated its account for a lengthy amount of time. This supports the sixth *Halberstam* factor, duration of assistance, and implicitly allows for more revenue sharing. Social media companies do a good job of removing terrorism-related content from their platforms,[176] but if this particular account went undetected while similar accounts were removed, the court might hold that against the social media company. If the plaintiffs also propose an independent duty for social media companies to not provide material support to FTOs, the claim would be even stronger. Fourth, the eventual perpetrator of the attack interacts with the FTO's social media account(s) and is radicalized through continued interaction. Last, the radicalized individual conducts a terrorist attack through the direction of the FTO. It will be difficult to plausibly allege that the FTO authorized the attack without discovery, as these directions will likely be communicated through private messages. It is still possible to allege if the perpetrator tells

---

[174] *See* Atchley v. AstraZeneca, 22 F.4th 204, 222 (D.C. Cir. 2022).

[175] *See, e.g.*, Chloe West, *How Much do YouTubers Make?–A YouTuber's Pocket Guide [Calculator]*, INFLUENCER MKTG. HUB (Jan. 25, 2024), https://influencermarketinghub.com/how-much-do-youtubers-make/ [https://perma.cc/PY7R-4CYY].

[176] *See infra* Part V.

someone else of his or her involvement with the FTO or posts a coded message before committing the attack.

Is this hypothetical allegation enough to withstand a motion to dismiss? The hypothetical relies heavily on the "substantial" side of the "knowing and substantial assistance" sliding-scale. The only argument on the knowledge side would be that it was reckless for the social media company not to remove the revenue-generating account for such a long period of time, but that theory is unproven. On the substantial side, the social media company would have provided monetary support to the FTO, a platform from which to recruit, and a communication system to plan and authorize the attack. Still, it seems unlikely that a court would find that the level of substantial assistance, with little to no knowledge, would rise to the level of culpability. Absent extreme circumstances, it is unlikely for JASTA to provide an avenue for secondary liability against a social media company.

V. ISSUES CURRENT CIVIL AIDING AND ABETTING THEORY IS NOT EQUIPPED TO ADDRESS

A. Size and Automation as a Shield

The *Twitter* opinion emphasizes the size and automation of social media companies in explaining that providing a platform for FTOs to promote terrorist ideologies, recruit new members, and even plan terrorist attacks does not necessarily make social media companies "culpable." The Court in *Twitter* is correct in stating that social media companies service billions of users, and when an FTO is one of those users, the company's relationship with the FTO is "arm's length, passive, and largely indifferent."[177] This consideration is important to prevent "mostly passive actors like banks [from becoming] liable for all of their customers' crimes by virtue of carrying out routine transactions."[178] It is primarily the size and automation of social media companies that make the facts of these cases a "far cry"[179] from those in *Halberstam* and create a shield for social media from aiding and abetting liability.

Social media provides far more utility to FTOs than phones, but in a similar way to purchasing a phone, social media companies are allowed to permit users to join and post content "without much (if any) advance screening."[180] The Court noted a counterfactual to how social media typically functions when pointing out that "if a platform consciously and selectively chose to promote content provided by a

[177] Twitter v. Taamneh, 598 U.S. 471, 500 (2023).

[178] *Id.* at 491.

[179] *Id.* at 487.

[180] *Id.* at 480.

particular terrorist group, perhaps it could be said to have culpably assisted the terrorist group."[181]

To further illustrate how automation shields social media companies, imagine a social media site that allowed anyone to create an account and view content, but restricted the ability to post content, send messages, or receive ad revenue to certain users. If the only user with these capabilities was a terrorist organization, it would be difficult to argue that the social media site maintained a passive or indifferent relationship with the terrorist organization. While the social media company's assistance to the terrorist organization may not have a "concrete nexus" to any individual attack, a victim could plausibly argue that the social media company "intentionally associated themselves" with the terrorist group and therefore "aided and abetted each and every . . . terrorist act committed."[182] These facts fall much closer to those in *Halberstam*. Although Hamilton herself did not have a concrete nexus to Welch's crimes, Hamilton's assistance "substantially helped Welch commit personal property crimes," which foreseeably led to Halberstam's death.[183] In this hypothetical, the social media's assistance would substantially help the terrorist organization radicalize new members, obtain funding, and plan future attacks.

To demonstrate how size affects the analysis, consider a slight alteration to the facts in *Halberstam*. Instead of a live-in partner assisting a burglar, what if the burglar instead employed a shady accounting business that frequently performed incomplete bookkeeping, made checks payable to the business, and falsified tax returns for millions of customers? Perhaps the accounting business would be guilty of many crimes, but because it provided these services passively and indifferently to many parties, it would be more difficult to allege the business was "consciously trying to help or otherwise participate in"[184] the burglaries, similar to Huawei in *Zobay*.[185] Phrased differently, the size of the operation would make it difficult to show the accounting business was aware that it assumed a role in illegal activities.[186] A victim might argue that the business was providing routine services in an unusual way. But it is not clear if "usual" refers to what is typical for the provider or what is typical for the services.[187] The size of the business's operation

---

[181] *Id.* at 502.

[182] *Id.* at 501–02.

[183] *Id.* at 487.

[184] *Id.* at 500 (internal quotations omitted).

[185] *See supra* Part III.B.2.

[186] *See* Linde v. Arab Bank, 882 F.3d 314, 329 (2d Cir. 2018) (finding that knowingly supporting an organization does not necessarily indicate a particular act was knowingly supported).

[187] *See infra* Part IV.B.

may protect it from aiding and abetting liability in any individual crime, as long as the business intentionally stayed ignorant of its customers' dealings.

It is unclear, then, exactly how large or passive a company must be for the actions of their users to be too far attenuated to constitute aiding and abetting. Perhaps precisely where this line falls is less important than illustrating the catch-22 for holding social media companies liable for aiding and abetting: as size and automation of social media increases, the usefulness of the social media to FTOs also increases. Fewer restrictions on user ability to join, post content, and interact with other users leads to larger, more interconnected social media sites from which FTOs have a larger audience to recruit. More automation also separates the social media companies from the FTO, making it more difficult to show knowing and substantial assistance.

B. How to Treat Recommendation Algorithms

Recommendation algorithms further assist "The Net"[188] by matching users who have viewed similar content to FTO messaging, helping FTOs reach their target audience in ways they themselves are unable to coordinate. Are recommendation algorithms passive and simply part of the platform, or is matching users with content an act performed by the social media company? Whether recommendation algorithms constitute passive or active assistance highlights how new technologies pose difficult questions for the law.

The plaintiffs in *Twitter* argued that these recommendation algorithms "go beyond passive aid and constitute active, substantial assistance."[189] The Court disagreed, stating that the "algorithms are merely part of" the social media infrastructure and "appear agnostic as to the nature of the content."[190] In this way, the Court determined it was better to treat social media companies like traditional service providers.

The discussion surrounding how to view recommendation algorithms has divided judges in the lower courts. Both *Force v. Facebook*[191] and *Gonzalez* considered whether recommendation algorithms constitute publishing for the purposes of the CDA, which prevents websites from being liable for content posted on their platform. Both courts held that recommendation algorithms have CDA immunity, with notable discussion. The concurrence in *Force* argues that recommendation

---

[188] *See supra* Part II.

[189] *Twitter*, 598 U.S. at 499.

[190] *Id.*

[191] 934 F.3d 53 (2d. Cir. 2019).

algorithms *proactively* create networks of people.[192] Judge Katzmann illustrates the point with the following hypothetical:

> Suppose that you are a published author. One day, an acquaintance calls. "I've been reading over everything you've ever published," he informs you. "I've also been looking at everything you've ever said on the Internet. I've done the same for this other author. You two have very similar interests; I think you'd get along." The acquaintance then gives you the other author's contact information and photo, along with a link to all her published works. He calls back three more times over the next week with more names of writers you should get to know.
>
> Now, you might say your acquaintance fancies himself a matchmaker. But would you say he's acting as the *publisher* of the other authors' work?[193]

Under Judge Katzmann's interpretation of how recommendation algorithms operate, it is difficult to say they are passive. Judge Katzmann continues to explain that the plaintiffs' claims did not "rely on treating Facebook as the publisher of others' information. Instead, they would hold Facebook liable for its *affirmative role* in bringing terrorists together."[194]

Whether recommendation algorithms constitute "publishing" or providing knowing and substantial assistance are admittedly different inquiries. But the discussion highlights how social media pushes the limits of how courts view traditional roles. Neither the CDA nor the common law of aiding and abetting developed while social media was prominent, and it is difficult to characterize social media through those lenses. The difficulty of applying pre-internet law to recommendation algorithms is compounded by the lack of clarity around the details of how these algorithms work.[195]

C. Lone Wolf Attacks

As described above, terrorist organizations often implement a four-step process for recruitment and radicalization over social media.[196]

---

[192] *Id.* at 83 (Katzmann, J., concurring in part and dissenting in part) (emphasis added).

[193] *Id.* at 76 (Katzmann, J., concurring in part and dissenting in part).

[194] *Id.* at 77 (Katzmann, J., concurring in part and dissenting in part) (emphasis added) (internal quotations omitted).

[195] *See* Arvind Narayanan, *Understanding Social Media Recommendation Algorithms*, KNIGHT FIRST AMEND. INST. COLUM. UNIV. (Mar. 9, 2023), https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms [https://perma.cc/QNM4-74LK].

[196] *See supra* Part II.

Recently, "Lone Wolf" attacks have been more common. Lone Wolf attacks refer to when an individual is exposed to "The Net" and becomes radicalized with minimal additional action from the FTO.[197] This is made possible primarily due to the tendency for social media to create echo chambers.[198] Vulnerable individuals may enter a community of terrorists and take violent action with little encouragement or guidance from the FTO, as many of the resources in "The Activation" are accessible to users who seek them out.

JASTA requires that the act of "international terrorism" from which relief is sought is (1) "committed, planned, or authorized" (2) "by an organization that had been designated as a foreign terrorist organization."[199] These two requirements notably limit the remedies for victims of terrorist acts.

In *Retana v. Twitter*, victims of a Dallas mass shooting sued Twitter, alleging that the shooter was radicalized by Hamas, an FTO, over Twitter, which led him to commit the act of violence.[200] It was determined that the perpetrator was a "self-radicalized shooter who merely 'liked' the Facebook pages . . . that had communicated with Hamas."[201] The Fifth Circuit held, "[w]e cannot conclude that the Dallas shooting transcended national boundaries. . . [the shooter] might have been radicalized in part by Hamas, but Hamas did not plan the shooting or even take credit for it."[202]

Even when an FTO does take credit for an attack, that is still not sufficient itself to establish that the attack was connected to the FTO. *Crosby v. Twitter* handled the 2016 Pulse Night Club shooting which resulted in 49 dead and 53 injured.[203] Shortly after the attack, ISIS took credit for the shooting.[204] An FBI investigation determined that the shooter became self-radicalized through ISIS internet content over several years.[205] Victims pursued legal action under a theory that the shooter was acting as an extension of the FTO across borders.[206] The court determined that ISIS had no real relationship to the shooter and

---

[197] *See Low Cost, High Impact: Combatting the Financing of Lone-Wolf and Small-Scale Terrorist Attacks: Hearing Before the Subcomm. on Terrorism and Illicit Finance, House Financial Services Comm.*, 115th Cong. 5 (2017) (statement of Dr. Matthew Levitt, Director, Stein Program on Counterterrorism and Intel., Wash. Inst. for Near East Pol'y).

[198] *See* Quattrociocchi, *supra* note 25.

[199] 18 U.S.C. § 2333(d)(2).

[200] *Retana v. Twitter*, 1 F.4th 378, 380 (5th Cir. 2021).

[201] *Id.* at 382.

[202] *Id.* at 381–82.

[203] 303 F. Supp. 3d 564, 569 (E.D. Mich. 2018).

[204] *Id.*

[205] *See id.*

[206] *See id.* at 572.

was merely "post[ing] information on the Internet."[207] It concluded "there are no plausible allegations at all that there was any tangible connection between ISIS and the Pulse Night Club shooting attack, or between [the shooter] and the defendants."[208]

Sinclair for Tucker v. Twitter[209] is another example of a case in which the terrorist organization took credit for an international attack. The plaintiffs were victims of a terrorist attack that involved a car driving through a crowded area in Barcelona.[210] The attacker was allegedly radicalized by ISIS over social media, and ISIS took credit for the attack.[211] The court's aiding and abetting analysis focused on whether the social media companies assisted "'*the person* who committed' the terrorist act."[212] *Twitter* indicates that the analysis is not quite correct,[213] but the court ultimately found that the plaintiffs did not plausibly allege that the social media companies knowingly provided substantial assistance to either the attacker or ISIS.[214]

These cases highlight a gap in the coverage of JASTA claims. While many factors contribute to an individual's self-radicalization, civil aiding and abetting liability does not effectively encourage social media companies to prevent attacks from self-radicalized individuals.

D. The Cycle of Detection, Suspension, and New Account Creation

The cases and discussion thus far have implied a cynical take on social media companies. It is important to clarify that social media companies do not want terrorist organizations to use their platforms, and they do not benefit from terrorists carrying out attacks. Consequently, they take significant steps to remove FTO content. For example, in 2018, Facebook claimed "it [found] and remove[d] 99 percent of ISIS- and al Qaeda-related content before users report[ed] it, thanks to a combination of photo and video matching software and human monitors."[215] Due to the massive amount of content these sites handle, however, it is

---

[207] *Id.*

[208] *Id.* at 575.

[209] No. C 17-5710 SBA, 2019 WL 10252752 (N.D. Cal. Mar. 20, 2019).

[210] *Id.* at *1.

[211] *Id.*

[212] *Id.* at *5.

[213] *See supra* Part III.A.2.

[214] *Sinclair*, 2019 WL 10252752, at *6.

[215] Larry Greenemeier, *Social Media's Stepped-Up Crackdown on Terrorists Still Falls Short*, SCI. AM. (July 24, 2018), https://www.scientificamerican.com/article/social-medias-stepped-up-crackdown-on-terrorists-still-falls-short/ [https://perma.cc/N9TS-HK8V]. It should be noted that this data may be somewhat misleading because it is unlikely that FTO-affiliated users would report terrorist content, and the echo chamber effect may prevent this content from reaching users that would report it.

nearly impossible that some material does not "slip through the cracks."[216]

Further exacerbating the problem of detection is that foreign terrorist organizations follow a common mantra: if at first you don't succeed try, try again. The cycle of detection, suspension, and creating new accounts was described in *Crosby*:

> Any ISIS accounts that the defendants do disable rapidly reappear within hours or days under simple reiterations of the same formulaic account handles used by previous accounts that were banned (e.g., accounts named "DriftOne00147" through "DriftOne00151" serially created, posting substantially the same messages, after accounts "DriftOne00146" through "DriftOne00150" were deleted).[217]

Even if social media companies are doing all they can to remove terrorist content from their platforms, it is difficult to overcome persistence from the FTOs. The obstacles of new account creation and massive content volume are problems that JASTA did not intend to battle. By pointing to *Halberstam* as the framework for aiding and abetting liability, Congress indicated it had in mind a far different situation of aiding and abetting; a large corporation with millions of users trying to fend off thousands of bad actors is indeed a "far cry" from the willful ignorance that indirectly assisted Hamilton in *Halberstam*.

Purely governmental regulation—especially through indirect means, such as secondary civil liability—poses many issues. A better solution to incentivize social media companies to combat terrorism might exist outside the legal system through self-regulation by social media companies and industry-wide organizations.[218] This could take the form of "private industry-level organizations creat[ing] rules and standards with which individual industry actors voluntarily comply."[219] Self-regulation would be a complex undertaking, as social media companies vary significantly in size and practice. Some emphasize peer-to-peer interaction, while others focus on information searching or data collection.[220] Skeptics may argue that self-regulation is akin to asking the fox to guard the henhouse, and the law must step in to force social media companies to increase their efforts to deter FTO usage. But

---

[216] *Id.*

[217] Crosby v. Twitter, Inc., 303 F. Supp. 3d 564, 568 (E.D. Mich. 2018).

[218] *See* Newton Minow & Martha Minow, *Social Media Companies Should Pursue Serious Self-Supervision–Soon: Response to Professors Douek and Kadri*, 136 HARV. L. REV. F. 428, 432–433 (2023).

[219] *Id.* at 433.

[220] *Id.* at 438–439.

current laws are ill-equipped to place significant pressure on social media companies. Outcomes would certainly improve if the social media industry coordinated standards for detection of terrorist activities and modification of recommendation algorithms to prevent the rapid spread of terrorist content in the first place.

VI. CONCLUSION

The Supreme Court's analysis in *Twitter* sheds light on how courts should approach aiding and abetting claims against social media companies. Furthermore, the Court's analysis implies that a less attenuated set of circumstances might create liability. After evaluating *Twitter* and aiding and abetting in other contexts, this Comment argues that, barring an exceptional set of facts, it is unlikely for plaintiffs to successfully bring a secondary liability claim against a social media company. While JASTA may not deter social media companies from further preventing the spread of terrorist activities on their platforms, the utility of social media platforms will continue to increase, leading to more deaths. Perhaps alternative solutions are better equipped to tackle these problems than the threat of aiding and abetting liability.