Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 37 | Issue 3 Article 2

4-16-2021

SOCIAL SUPPORT FOR TERRORISTS: FACEBOOK'S "FRIEND SUGGESTION" ALGORITHM, SECTION 230 IMMUNITY, MATERIAL SUPPORT FOR TERRORISTS, AND THE FIRST AMENDMENT

Yost, Ellen Smith

SOCIAL SUPPORT FOR TERRORISTS: FACEBOOK'S "FRIEND SUGGESTION" ALGORITHM, SECTION 230 IMMUNITY, MATERIAL SUPPORT FOR TERRORISTS, AND THE FIRST AMENDMENT

By Ellen Smith Yost[1]

Victims of international terrorism have recently argued that Facebook incurs civil liability under the material support provisions of the Anti-Terrorism Act (ATA) when its "friend suggestion" computer algorithm mines user data, identifies radicalized users with an interest in terrorism, and suggests that these users become "friends" with terrorist groups like Hamas that communicate over the platform. Under Section 230 of the Communications Decency Act (Section 230), social media companies like Facebook are currently immune from most "material support to terrorists" claims. But material support claims based on Facebook's algorithms are novel and different. This article considers, for the first time, the statutory and constitutional hurdles facing plaintiffs bringing algorithmic material support claims. Section 230 reform is currently the subject of intense regulatory and legislative interest. A terrorism carve-out is one proposed reform. For this reason, it is increasingly important for social media companies, litigants, courts, and Congress to understand the intersecting statutory and constitutional issues presented by algorithmic material support claims.

First, such plaintiffs face the statutory hurdle posed by Section 230. Currently, circuits are split on the existence and scope of immunity granted by Section 230. The limited "definitional" interpretation of § 230(c)(1) favored by the Seventh Circuit, unlike the broad "immunity" approach currently favored by many circuits, appropriately balances the competing policy concerns reflected in Section 230 and in statutes like the ATA. The definitional approach to Section 230 does not bar algorithmic material support claims against social media platforms. Next, plaintiffs face a statutory hurdle posed by the ATA's proximate causation requirement. Social media companies that worry about a flood of material support claims if Section 230 immunity is scaled back by Congress or the courts should find this hurdle's presence reassuring. The ATA's proximate cause requirement will bar all but the strongest, most meritorious algorithmic material support claims—an outcome that is fair to

[1] JD Candidate, SMU Dedman School of Law, 2021. The author would like to express her gratitude to Jeffrey Kahn, Altshuler Distinguished Teaching Professor and Professor of Law at SMU Dedman School of Law, for his support and comments on a draft of this article. Any errors are the author's alone.

plaintiffs and to social media companies. Finally, if algorithmic material support claims are not statutorily barred, they are likely barred by the First Amendment. As the work of First Amendment scholar Stuart Minor Benjamin suggests, Facebook's friend suggestion algorithm is likely to be protected speech. Under the Supreme Court's decision in Holder v. Humanitarian Law Project, the civil provisions of the Anti-Terrorism Act therefore could not be constitutionally applied to this algorithmic speech, no matter how meritorious the claim.

CONTENTS

INTRODUCTION: *FORCE V. FACEBOOK*

A client tells you her tragic story.[2] A U.S. citizen, she lives in Israel. One terrible day, as she disembarked at a Jerusalem rail station with her three-month-old daughter, a member of the Palestinian terrorist group Hamas rammed his vehicle into the crowd, violently striking the baby's stroller and its helpless occupant. The baby died two hours later. Seeking justice and compensation for your client, you consider who might bear civil liability under U.S. law for this heinous attack. The attacker himself was killed and had, in any case, no money. You can sue Hamas under the civil damages provision of the Anti-Terrorism Act (ATA).[3] But collecting damages from a foreign terrorist group is difficult to impossible.[4] Fortunately, your client can also assert civil claims under the ATA against any U.S. entity that has provided material support to Hamas.[5] The social media company Facebook arguably provides such support and is a tempting target.[6] Of course, you need to understand your likelihood of success on such a claim. To do this, you must answer these questions: Is Facebook potentially liable to victims of terrorism, under the statute criminalizing material support to terrorists, when the company's algorithms enable the responsible terrorist group's actions by introducing it to potential new members? Or is the company exempt from liability under either Section 230 of the Communications Decency Act of 1996 (CDA) or the First Amendment?

---

[2] Sadly, this hypothetical scenario is based on the tragic death of Chaya Zissel Braun. Braun's family were among the plaintiffs in Force v. Facebook, Inc., 934 F.3d 53, 57–58 (2d Cir. 2019).

[3] *See, e.g.*, Rubin v. Hamas-Islamic Resistance Movement, No. CIV. A. 02-0975 (RMU), 2004 WL 2216489, at *4 (D.D.C. 2004) (granting default judgement and damages to victims of Hamas terrorist attack). Our hypothetical attorney can also sue state sponsors of Hamas' terrorism under § 1605A of the Foreign Sovereign Immunities Act (FSIA). *See also* Braun v. Islamic Republic of Iran, 228 F. Supp. 3d 64, 87 (D.D.C. 2017) (ordering Iran and Syria to pay $178,500,000 in damages to the family of Chaya Zissel Braun).

[4] *See, e.g.*, Mica Rosenberg, *Suing Governments over Terror no Sure Thing Despite U.S. September 11 Law*, REUTERS (Sept. 29, 2016), https://www.reuters.com/article/us-usa-sept11-lawsuits-analysis/suing-governments-over-terror-no-sure-thing-despite-u-s-september-11-law-idUSKCN11Z326.

[5] *See, e.g.*, Force, 934 F.3d at 61.

[6] *See id.*

The Supreme Court recently declined an opportunity to address these questions in *Force v. Facebook*.[7] This was a mistake. The questions above implicate some of the most important legal and social issues facing U.S. society today, like how to balance free speech, liability, and harm in online forums; and how legal structures can provide incentive for internet companies to safeguard users and third parties while ensuring these companies have freedom to innovate and thrive in a competitive global marketplace. For this reason, the Court should take its earliest opportunity to decide the scope of Section 230 and its relationship to the Anti-Terrorism Act and other statutes. This article tackles the questions the Court should have answered in *Force*. As Section 230 is currently the subject of intense regulatory, legislative, and scholarly interest, and a terrorism carve-out is one of several recently proposed reforms to Section 230, it is increasingly important that litigants, courts, and Congress understand these interrelated issues.[8]

In *Force*, U.S. citizens who lost loved ones in Hamas terrorist attacks sought civil damages from Facebook, which they claimed unlawfully provided material support to a designated foreign terrorist organization and its murderous members.[9] The *Force* plaintiffs based their claims on provisions of the ATA found at 18 U.S.C. §§ 2333, 2339A, and 2339B.[10] The Second Circuit rejected these claims, granting Facebook's Motion to Dismiss and finding that Facebook was immunized from such suits under Section 230(c)(1) of the CDA.[11] Section 230(c)(1) provides 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," which courts including the Second Circuit interpret as providing companies like Facebook immunity from many civil claims.[12]

---

[7] Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020) (mem.).

[8] *See infra* notes 236, 237, 238 and accompanying text.

[9] *See* Force, 934 F.3d at 57.

[10] *See infra* Section II. C. notes and accompanying text.

[11] *See* Force, 934 F.3d at 57; 47 U.S.C. § 230; The "Communications Decency Act," was enacted in 1996. *See* Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, § 509, 110 Stat. 137, 138–39 (1996); *see generally* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

[12] *See, e.g.*, Force, 934 F.3d at 63–64; *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998). However, § 230 provides no defense to criminal liability under the ATA. 47 U.S.C. § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of . . . any other Federal criminal statute."). So, the government

So far as the Second Circuit's decision applies Section 230 to civil material support claims based on social media content posted by Hamas or its members, the result is uncontroversial.[13] However, the *Force* plaintiffs also brought novel claims based on Facebook's "friend suggestion" algorithm.[14] This algorithm is a proprietary computer program, developed by Facebook's coders, that generates notifications suggesting users "friend" other selected users, based upon users' shared interests (as identified by Facebook) and other factors.[15] And as Chief Judge Robert Katzmann of the Second Circuit argued in a partial dissent to the *Force* opinion, § 230(c)(1) arguably does not immunize Facebook from these claims, since the relevant content generated by this algorithm was not "provided by another user" as the statute requires, but created by Facebook itself.[16]

Facebook, Judge Katzmann argued, could be liable under § 230(c)(1) for suits based on the site's algorithmically generated content—the "friend suggestions"—if the algorithm, as the *Force* plaintiffs claimed, mines user activity on the site, analyzes data points like users' "likes" and clicks, and then "suggests" friends and other content a user might enjoy.[17] The algorithm identifies people with terror-related interests and suggests they become friends with existing Hamas members, essentially sending Hamas eager new recruits.[18]

---

would not be similarly barred by § 230(c)(1) from bringing criminal material support charges against Facebook.

[13] *See, e.g.*, Crosby v. Twitter, Inc., 303 F. Supp. 3d 564, 568 (E.D. Mich. 2018), *aff'd*, 921 F.3d 617, 627 (6th Cir. 2019). *See also* KOSSEFF, *supra* note 11, at 228–38 (discussing Fields v. Twitter, Inc., 217 F. Supp. 3d 1116 (N.D. Cal. 2016), *aff'd* 881 F.3d 739, 750 (9th Cir. 2018). As Kosseff notes, the district court in *Fields* held that the CDA barred the plaintiffs' material support claims. The Ninth Circuit, however, declined to reach the CDA question, instead affirming the lower court's dismissal for lack of proximate cause.

[14] *See* Force, 934 F.3d at 77 (J. Katzmann, dissenting).

[15] *See id.*

[16] *See id.*

[17] *See id.*

[18] In the past, Facebook has closely guarded the details of its proprietary algorithms' actual function. *See* Will Oremus, *Who Controls Your Facebook Feed*, SLATE (Jan. 3, 2016), http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html (2016 article discussing the secret nature of Facebook's newsfeed algorithm; the *Force* plaintiffs brought claims based on incidents in 2014 and 2016.). Since the *Force* plaintiffs' claims were dismissed prior to discovery, their allegations as to the friend suggestion algorithm's function at the time remain untested. *See* Force, 934 F.3d at 61–62. This article accepts the *Force* plaintiffs' allegations for purposes of discussion only.

Facebook, the *Force* plaintiffs said, knows that its algorithmic programming choices cause this result, yet has failed to adjust the algorithm to eliminate the recruitment effect.[19] This, they claimed, is providing support to international terrorists as defined in 18 U.S.C. §§ 2239A or 2239B.[20] By violating the material support provisions, Facebook becomes liable under the ATA's civil cause of action, found at 18 U.S.C. § 2333.[21]

This novel algorithmic argument leads to a novel issue: the constitutionality of the ATA's material support provisions as applied to Facebook's algorithm. Because courts have previously resolved all civil material support claims against social media companies like Facebook on statutory grounds under either Section 230 or § 2333, no court has yet addressed the question of whether §§ 2339A, 2339B, and 2333 could be permissibly applied to an algorithm like this, which may be "speech" protected by the First Amendment.[22] Only if the statute's civil cause of action and the underlying criminal provisions, as applied to this algorithm, are constitutional will plaintiffs like those in *Force* realize an opportunity to seek relief on the merits.[23]

In sum, victims of international terrorism bringing civil material support claims against social media companies like Facebook must clear two preliminary hurdles, which this article examines. First, there is a question of statutory immunity under § 230(c)(1) of the Communications Decency Act.[24] This is the question addressed in *Force*. Second, there is a question of whether the First Amendment prevents Congress from regulating the algorithm at issue.[25]

---

[19] *See* Force, 934 F.3d at 77 (J. Katzmann, dissenting).

[20] *Id.* at 61 (plaintiff's claims under §2333); *see infra* note 21 (describing the relationship between §2333 and §2339A and B).

[21] Plaintiffs (like those in *Force*) bringing material support-theory claims against U.S. companies under § 2333's JASTA-added secondary liability provisions must essentially step into the shoes of the government and prove that the company is guilty of violating § 2339A or § 2339B. Once such a violation is established, it serves as the basis for and supplies the *mens rea* required by § 2333. *See* Maryam Jamshidi *How the War on Terror Is Transforming Private U.S. Law,* 96 WASH. U.L. REV. 559, 576–91 (2018) (listing cases proceeding on this theory and explaining the relationship between § 2333 and § 2339A–B in detail).

[22] *See* Crosby, 303 F. Supp. 3d at 568; *see also* Retana v. Twitter, Inc., 419 F. Supp. 3d 989, 989–95 (N.D. Tex. 2019). On the threshold question of whether Facebook's algorithmic question is "speech" protected by the First Amendment and, if so, how robustly, *see infra* Section III.

[23] *See infra* Section II.C. (discussing Holder v. Humanitarian Law Project).

[24] *See* Force, 934 F.3d 53 at 61; *see infra* Section I.C.

[25] *See infra* Section II.

Assuming for purposes of this analysis that the claims raised in *Force* about the operation and effect of Facebook's friend suggestion algorithm are true, this article first considers statutory hurdles. It argues that the text and purpose of § 230(c)(1) and (2) together reflect Congress' desire to protect companies from defamation-type suits, encouraging them to engage in content filtering and removal. To reflect this purpose, the Court should adopt a limited "definitional" interpretation of § 230(c)(1), favored by the Seventh Circuit.[26] This article rejects the broad "immunity" approach favored by many circuits as unsupported by the text of the statute, in structural and historical context, and as granting overbroad protection. The definitional approach to § 230(c)(1) does not bar algorithmic material support claims like those raised by the *Force* plaintiffs.[27] Though companies like Facebook would no doubt prefer a total immunity interpretation, they need not fear unfair ruinous liability under the material support statute's civil provisions, the Anti-Terrorism Act's proximate cause requirement will still bar all but the most meritorious claims. [28]

Next, this article examines the constitutional hurdle. First, it considers whether Facebook's friend suggestion algorithm is constitutionally protected speech. Applying the work of First Amendment scholar Stuart Minor Benjamin, it concludes that this algorithm is constitutionally protected speech, because (1) Facebook's programmers, at the direction of its CEO, direct this algorithm to find and prioritize certain user data, which it analyzes to create new content—the friend suggestions, and (2) the algorithm communicates Facebook's message that increased social interaction is desirable.[29] Finally, it considers whether the material support statute is unconstitutional as applied to civil claims based on Facebook's algorithms. Applying the Supreme Court's reasoning in *Holder v. Humanitarian Law Project* to the facts alleged in *Force*, it concludes that the ATA's civil liability provision cannot constitutionally be applied to Facebook's algorithmic speech.[30] The article concludes by considering potential reforms to Section 230, including a proposed terrorism carve out. This would prevent Section 230 from being used as a defense to liability under the ATA, raising the constitutional issue this article identifies.

---

[26] *See infra* Section I.B.
[27] *See infra* Section I.C.
[28] *See infra* Section I.C.
[29] *See infra* Section II.A.
[30] *See infra* Section II.C.

I. THE STATUTORY HURDLES: CDA SECTION 230, THE ATA, AND FACEBOOK'S "FRIEND SUGGESTION" ALGORITHM

Section 230 of the Communications Decency Act (CDA) of 1996 is the first hurdle plaintiffs like those in *Force* must clear.[31] In their petition for cert, the *Force* plaintiffs asked the Court to resolve a circuit split regarding the type and scope of immunity granted to social media platforms under § 230(c)(1).[32] Under the broadest form of the majority "immunity" approach (employed in *Force* by the Second Circuit), any civil claim against Facebook that is even *indirectly* based on user content is barred.[33] This includes the *Force* plaintiffs' algorithm-based claims. Alternatively, if the Court adopts the minority "definitional" approach to § 230(c)(1), which holds that this subsection merely blocks treating an internet content provider as a "speaker or publisher," their claims would not be barred.[34] This approach is taken by the Seventh Circuit.[35] This part of the article will examine this circuit split in detail after taking a closer look at the statutory language itself and the legislative history. It recommends the definitional approach preferred by the Seventh Circuit as the better view but also examines whether, under the Second Circuit's immunity approach, the *Force* plaintiffs' claims are necessarily barred.

---

[31] *See* Force, 934 F.3d at 61.

[32] *Cf.* the "immunity approach" circuits: *See* Force, 934 F.3d at 53; Jane Doe No. 1 v. Backpage.com, 817 F.3d 12, 18–20 (1st Cir. 2016); Green v. Am. Online (AOL), 318 F.3d 465, 470 (3d Cir. 2003); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997); Doe v. MySpace, Inc., 528 F.3d 413, 418 (5th Cir. 2008); Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 406–10 (6th Cir. 2014); Johnson v. Arden, 614 F.3d 785, 792 (8th Cir. 2010); Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1176–88 (9th Cir. 2008) (en banc); Silver v. Quora, Inc., 666 Fed. App'x 727, 728–29 (10th Cir. 2016); Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1324 (11th Cir. 2006) (with the "definitional approach" articulated in Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 681, 693–98 (N.D. Ill. 2006), *aff'd sub nom.* Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669–72 (7th Cir. 2008). The Ninth Circuit, however, is moving closer to the definitional approach. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100–01 (9th Cir. 2009)).

[33] *See infra* Section II.A.; *see also* Force, 934 F.3d at 64. A petition for panel rehearing or, alternatively, rehearing en banc was denied. Order, Force, No. 18-397, 2019 at 2–3 (2d Cir. 2019). As noted previously, § 230 does not immunize Facebook from criminal liability under §§ 2339A–B. *See* 47 U.S.C. 230(e)(1).

[34] Force, 934 F.3d at 62.

[35] *See* Chicago Lawyers, 461 F. Supp. 2d at 693–98.

A. The CDA and the ATA: two statutes with diverging purposes

Considering the legislative history and purpose of the ATA and the CDA helps us understand whether, how, and why the CDA might exempt Facebook from civil liability under the ATA. The legislative history of the ATA reflects Congress' effort to expand ways to hold terrorists and their supporters liable.[36] The legislative history of the CDA reflects Congress' desire to protect two distinct constituencies: internet users and internet companies.[37] The claim at issue in *Force* thus presents an interpretive dilemma. Expansive interpretation of the ATA raises liability for internet companies whom the CDA seeks to protect, while expansive interpretation of the CDA deprives sympathetic terror victims of a potentially powerful cause of action.

The ATA, found at 18 U.S.C. §§ 2331-2339, provides civil and criminal causes of action against foreign terrorists. Section 2333, the civil cause of action for victims of terrorist acts, dates to 1992.[38] Section 2239A, which criminalizes providing material support in aid of terrorist attacks, was added in 1994.[39] Section 2239B, which similarly criminalizes providing material support to a designated foreign terrorist organization, was added in 1996.[40] By the same legislation in 1996, Congress also amended and enlarged Section 2339A.[41] In 2016, Congress amended and broadened § 2333 through the Justice Against Sponsors of Terrorism Act (JASTA).[42] JASTA, the purpose of which was to "provide civil litigants with the broadest possible basis . . . to seek relief against [material supporters of terrorism]," added secondary liability for civil aiding and abetting, and for civil conspiracy, to § 2333.[43]

Most recently, Congress amended §§ 2331 and 2333 in 2018's Anti-Terrorism Clarification Act (ATCA), limiting exclusions from liability under the ATCA and expanding the ATCA's civil remedies

---

[36] *See infra* notes 39–48 and accompanying text (describing Congressional actions expanding the ATA's causes of action).
[37] *See infra* notes 60–62 and accompanying text.
[38] *See* Federal Courts Administration Act of 1992, Pub. L. No. 102-572, § 1003, 106 Stat. 4506, 4522.
[39] *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 120005, 108 Stat. 2022.
[40] *See* Antiterrorism and Effective Death Penalty Act (AEDPA), Pub. L. No. 104-132, § 303, 110 Stat. 1214, 1250 (1996).
[41] *See id.* § 323.
[42] *See* Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. 114-222, § 2(b), 130 Stat. 852, 853 (2016).
[43] *Id.*

and jurisdiction.[44] ATCA, like JASTA, was intended to help plaintiffs recover for injuries suffered at the hands of terrorists.[45] ATCA's amendments applied not just prospectively but to "any civil action pending on . . . the date of the enactment of this Act."[46] This unusual provision was the result of "active advocacy effort by plaintiffs who had received adverse decisions in existing terrorism-related civil litigation" and was "primarily intended to revive those plaintiffs' cases."[47] Thus, the recent history of the ATA reflects Congress' desire to increase terror victims' access to civil remedies. However, this intent to expand the statute's reach does not explicitly overrule the CDA. [48] Notably, the pending terrorism-based civil claims Congress revived by ATCA did *not* include terrorism-based civil material support cases against social media companies, though several such claims had been filed and dismissed under the CDA by that time, as Congress was surely aware.[49]

The CDA, now found at 47 U.S.C § 230, was enacted in 1996 as the internet first began to touch many Americans' lives.[50] As enacted, the CDA was comprised of two sections: § 223 and § 230.[51] Section 223, which courts swiftly deemed an unconstitutional restriction on users' First Amendment-protected rights, created protections to shield minor users from obscene or harassing content and

---

[44] *See* Anti-Terrorism Clarification Act (ATCA), Pub. L. 115-253, § 2(a), 132 Stat. 3183 (2018).
[45] *See* H.R. REP. NO. 115-858, at 2 (2018).
[46] ATCA, Pub. L. 115-253, §§ 2(b), 3(b), 132 Stat. 3183 (2018).
[47] *See* Harry Graver & Scott R. Anderson, *Shedding Light on the Anti-Terrorism Clarification Act of 2018*, LAWFARE (Oct. 25, 2018, 12:00 PM), https://www.lawfareblog.com/shedding-light-anti-terrorism-clarification-act-2018.
[48] The Second Circuit rejected the *Force* plaintiffs' claim that the 2016 JASTA amendments to § 2339A and § 2339B implicitly repealed § 230(c)(1). Force, 934 F.3d at 72 ("JASTA merely expanded Section 2333's cause of action to secondary liability; it provides no obstacle—explicit or implicit—to applying Section 230.").
[49] *See* Graver & Anderson, *supra* note 47; *see also* Crosby v. Twitter, Inc., 303 F. Supp. 3d 564, 568 (E.D. Mich. 2018), *aff'd*, 921 F.3d 617, 622 (6th Cir. 2019); Pennie v. Twitter, Inc., 281 F. Supp. 3d 874, 887 (N.D. Cal. 2017); Fields v. Twitter, Inc., 217 F. Supp. 3d 1116, 1120 (N.D. Cal. 2016), *aff'd*, 881 F.3d 739, 749–50 (9th Cir. 2018) (affirming dismissal on proximate causation without reaching the CDA issue).
[50] *See generally* KOSSEFF, *supra* note 11.
[51] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 § 501-09.

penalize internet providers for knowingly transmitting it.[52] According to its author, Senator James Exon, § 223's purpose was to make sure the "information superhighway" did not become a "red light district" where children would be accosted with "inappropriate communications" or citizens menaced by "uninvited indecencies."[53]

Section 230 was introduced as the "Online Family Empowerment" amendment to Senator Exon's legislation, by Representatives Chris Cox and Ron Wyden, who feared Exon's CDA would stifle online freedom and technological innovation.[54] It was a direct response to a court decision that had shaken the nascent internet industry, *Stratton Oakmont, Inc. v. Prodigy Services Company*.[55] In *Stratton Oakmont*, the internet company Prodigy was held liable as a "publisher" of defamatory statements posted by a user on its chat board.[56] Ironically, Prodigy's efforts to screen and remove such offensive content had exposed it to this liability.[57] As a factually similar case had recently found, an internet service provider could not be held liable as a publisher when it took *no* steps to police content on its chat boards.[58] *Stratton Oakmont* provided a strong disincentive for companies to establish and enforce content standards.[59]

---

[52] *See id.* § 502; *see also* Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 2329-30, 2340 (1997) (affirming lower court order enjoining the Government from enforcing the criminal provisions of § 223(a) and (d)).

[53] 141 Cong. Rec. S1953 (July 16, 1996); Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. at *53 (1996).

[54] *See* 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995). *See also* KOSSEFF, *supra* note 11, at 59–76.

[55] *See* 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (Cox stated, "Ironically, the existing legal system provides a massive disincentive for the people who might best help us control the Internet to do so," and comparing Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995), with Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991)); *see also* H.R. REP. No. 104-458, at 194 (1996) (Conf. Rep.) ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material."); *see also* KOSSEFF, *supra* note 11, at 45–56.

[56] *See supra* note 55.

[57] *See supra* note 55.

[58] *See* Cubby, 776 F. Supp. at 140.

[59] *See supra* note 55.

Beyond overruling *Stratton Oakmont*, Cox and Wyden's amendment had two purposes.[60] It aimed to "promote the continued development of the internet" by safeguarding the industry from burdensome state and federal regulation.[61] It also aimed to maximize users' control over what information they—and their children—received via the internet.[62] These purposes supported each other. Only if companies were free to innovate and satisfy diverse user preferences for "safe" (or unsafe) content would the internet continue to flourish, and only if companies were willing to provide such screening could users be effectively protected.[63] To this end, § 230(c), the operable portion of § 230, is titled "Protection for 'Good Samaritan' blocking and screening of offensive material" and is comprised of two subsections.[64] The first, § 230(c)(1), "Treatment of publisher or speaker," states in full that: "No 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."[65] The second, § 230(c)(2), "Civil liability," provides that "[n]o provider or user of an interactive computer service shall be held liable on account of" their voluntary good faith actions "to restrict access to or availability of" material the provider considers "objectionable,"[66] or their voluntary provision or enabling of content blocking or screening technologies.[67] Section 230 specifically excludes certain laws from its scope, notably intellectual property laws, criminal laws, and the

---

[60] *See* 47 U.S.C. § 230(b).
[61] *Id.*
[62] *Id.*
[63] *See* 141 Cong. Rec. H8468-69 (daily ed. Aug. 4, 1995) (Remarks of Rep. Cox: "Some have suggested . . . that we hire even more bureaucrats and more regulators who will attempt, either civilly or criminally, to punish people by catching them in the act of putting something into cyberspace. Frankly, there is just too much going on on the Internet for that to be effective. No matter how big the army of bureaucrats, it is not going to protect my kids because I do not think the Federal Government will get there in time . . . [we need] something that actually works.").
[64] 47 U.S.C. § 230(c).
[65] 47 U.S.C. § 230(c)(1).
[66] This includes material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2).
[67] 47 U.S.C. § 230(c)(2).

provisions of (invalidated) § 223.[68] The ATA's civil cause of action is not among these exclusions.[69]

Section 230(c)(1) is the provision at issue in *Force*. It confers protection from civil suits when three criteria are met.[70] First, the defendant must be a provider of an interactive computer service.[71] Second, the claims must be based upon information provided by another information content provider.[72] And third, the service provider must be being treated as the publisher or speaker of the information at issue.[73] Courts are split, however, on the scope and type of protection that § 230(c)(1) provides.[74] Some courts hold it confers broad immunity and use an expansive concept of "publication," while others hold it confers only limited immunity or functions as a "definitional" carve out for publication-based torts like defamation.[75] This section recommends the Court resolve this circuit split by adopting the Seventh Circuit's definitional approach to § 230(c)(1), as this limited approach provides appropriate protection for internet companies and respects the bounds of the CDA, as written. It then considers whether, under this or the majority immunity interpretation, § 230(c)(1) properly bars claims like those at issue in *Force*.

B. Resolving the current circuit split about what protection § 230(c)(1) grants to internet communication service providers like Facebook

Courts consistently find that Facebook is a provider of an interactive computer service potentially covered by § 230(c)(1).[76] But courts are split on the scope and type of protection § 230(c)(1) grants

---

[68] 47 U.S.C. § 230(e).

[69] *See id.* The Second Circuit rejected the *Force* plaintiffs' claims that because § 230 does not apply to criminal provisions, and § 2333 depends upon proving the underlying criminal violations in §§ 2339A or B, the CDA did not apply to their claims under § 2333. Force, 934 F.3d at 71.

[70] *See, e.g.*, Jones v. Dirty World Entertainment Recordings, LLC, 755 F.3d 398, 409 (3rd Cir. 2014).

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Cf.* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997), *with* Chicago Lawyers' Committee for Rights Under Civil Law, Inc. v. Craigslist, 519 F.3d 666, 669 (7th Cir. 2008).

[75] *See supra* note 74.

[76] *See, e.g.*, Klayman v. Zuckerberg, 753 F.3d 1354, 1355–60 (D.C. Cir. 2014); *see also* Sikhs for Justice, Inc. v. Facebook, Inc., 144 F. Supp. 3d 1088, 1093 (N.D. Cal. 2015), *aff'd*, 697 F. App'x 526 (9th Cir. 2017).

to service providers like Facebook.[77] A majority of courts hold that § 230(c)(1) gives internet providers immunity from any claim based on the activity of "publishing" third-party content.[78] Some courts consider this immunity broad, covering any civil claim based on the service's making information provided by a user available to others.[79] Other courts limit this immunity to claims based on a service's "exercise of traditional editorial functions."[80] Still others find that § 230(c)(1) defines limits on application of "publisher" liability.[81]

The immunity approach was established in *Zeran v. America Online (AOL)*.[82] *Zeran* involved malicious anonymous posts made to AOL's online "bulletin board."[83] The posts, made just a week after the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, advertised the sale of t-shirts bearing horribly "offensive and tasteless slogans" related to the attack.[84] Users were urged to call Ken Zeran to purchase these shirts.[85] After the unsuspecting and innocent Zeran was deluged with irate calls and threats, he reported the hoax posts to AOL.[86] Zeran repeatedly requested that AOL remove the posts, block the anonymous poster, and post a retraction. When his pleas went unanswered, he sued AOL for negligence and defamation.[87] AOL raised § 230 as a defense and moved for judgment on the pleadings, which the trial court granted.[88]

The Fourth Circuit's opinion affirming the lower court's decision made several bold assertions about § 230. First, the court stated, the "plain language" of § 230(c)(1) where "'[n]o provider or

---

[77] *See supra* note 74.

[78] *See* Backpage.com, 817 F.3d at 12; *see* Force, 934 F.3d at 53; *see* Green v. America Online (AOL), 318 F.3d at 465; *see* Zeran, 129 F.3d at 330–31; *see* MySpace, Inc., 528 F.3d at 413; *see* Jones, 735 F.3d at 406–07; *see* Johnson, 614 F.3d at 785; *see* Roommates.com, LLC, 521 F.3d at 1157; *see* Silver, 666 Fed. App'x at 727; *see* Almeida, 456 F.3d at 1316; Marshall's Locksmith Serv. Inc., v. Google, LL*C*, 925 F.3d 1263, 1267 (D.C. Cir. 2019).

[79] *See* Force, 934 F.3d at 64; *see* MySpace, Inc., 528 F.3d at 418; *see* Jones, 755 F.3d at 406–07.

[80] *See* Backpage.com, 817 F.3d at 18; *see* Barnes, 570 F.3d at 1101 (finding § 230 applied to a non-publication-based tort where the cause was essentially defamation, recast, and applying a "publication"-type analysis).

[81] *See* City of Chicago v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010).

[82] *See* Zeran,129 F.3d at 330.

[83] *See id.*

[84] *See id.*

[85] *See id.*

[86] At one point, "Zeran was receiving an abusive phone call approximately every two minutes." *Id.* at 329.

[87] *Id.* at 328.

[88] *See* Zeran,129 F.3d at 329–30.

user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider . . . creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[89] Specifically, it stated, this bars "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content."[90] Next, though it had declared the language "plain," the court considered the legislative intent behind § 230.[91] Focusing on § 230's internet service provider-protective purpose (while barely mentioning its customer-protective purpose) the court announced that § 230(c) should be interpreted "broadly," in favor of immunity for companies.[92] Applying this broad construction, the court held that AOL was immunized against the negligence and defamation claims.[93]

Zeran's dicta supports the broadest version of § 230(c)(1) immunity.[94] In dicta, the court stated that the Congressional anti-regulatory intent behind § 230(c) supported reading that provision as extending companies immunity to "tort."[95] Congress, the *Zeran* court said, "recognized the threat that *tort-based lawsuits* pose to freedom of speech in the new and burgeoning Internet medium."[96] In enacting § 230(c), Congress chose to deter harmful online content through "vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer," and not "through the separate route of imposing *tort liability* on companies that serve as intermediaries for other parties' potentially injurious messages."[97] Courts following a narrow immunity

---

[89] *Id.* at 330.
[90] *Id.*
[91] *But see* Caminetti v. United States, 37 S. Ct. 192, 194 (1917) ("Where the language is plain and admits of no more than one meaning, the duty of interpretation does not arise" and courts should look only to the text.).
[92] Zeran, 129 F.3d at 330.
[93] *Id.* at 335.
[94] *See* Force, 934 F.3d at 53; *see* MySpace, Inc., 528 F.3d at 418; *see* Jones, 755 F.3d at 406–07; *see* Almeida, 456 F.3d at 1321; *see* Marshall's Locksmith Serv., 925 F.3d at 1267.
[95] *See* Zeran, 129 F.3d at 330–31.
[96] *Id.* at 330 (emphasis added).
[97] *Id.* at 330–31 (citing § 230(b)(5)) (emphasis added).

approach, by contrast, look to *Zeran*'s more limited "traditional editorial functions" language.[98]

On the other side of the split is the Seventh Circuit, which considers § 230(c)(1) a "definitional provision" that provides no immunity.[99] Instead, the section "limits who may be called the publisher of information that appears online" and is a defense to liability under actions that depend upon status as a "publisher."[100] A Chicago district court, declining to follow the by then well-established *Zeran* approach, articulated this approach in *Chicago Lawyers' Committee For Civil Rights Under the Law, Inc. v. Craigslist, Inc.*[101] *Chicago Lawyers* involved a Fair Housing Act (FHA) challenge brought by a nonprofit group against Craigslist, an online classified ads site.[102] The group sought a declaratory judgment that Craigslist, by accepting and displaying housing ads that expressed an impermissible preference for certain tenants, violated provisions of the FHA.[103] The ads were posted by users through Craigslist's submission portal.[104] Craigslist claimed § 230(c)(1) immunized it from FHA liability, since the discriminatory ad content was provided by users.[105] "[T]en companies and trade associations affiliated with the online and electronic communications industries," including Amazon, Google, and Yahoo!, filed a joint amicus brief urging the court to adopt Craigslist's position.[106]

The district court acknowledged that "[n]ear-unanimous case law [following *Zeran*] holds that Section 230(c) affords immunity to [internet companies] against suits that seek to hold [them] liable for third-party content."[107] However, the court respectfully disagreed with *Zeran*'s broad reading of § 230.[108] "It is a fundamental canon of statutory construction," the district court noted, "that the words of a

---

[98] *See id.* at 330; *see also* Backpage.com, 817 F.3d at 12 (1st Cir. 2016); Barnes, 570 F.3d at 1101, *as amended* (Sept. 28, 2009) (finding § 230 applied to a non-publication-based tort where the cause was essentially defamation, recast, and applying a "publication"-type analysis).

[99] *See* StubHub!, Inc., 624 F.3d at 366.

[100] *See id.*

[101] Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc*.,* 461 F. Supp. 2d 681, 693 (N.D. Ill. 2006), *aff'd sub nom*. 519 F.3d 666 (7th Cir. 2008).

[102] Chicago Lawyers, 461 F. Supp. 2d at 686.

[103] *Id.* at 685–87.

[104] *Id.* at 684–85.

[105] *Id.* at 687.

[106] *Id.* at 683–84.

[107] *Id.* at 688.

[108] Chicago Lawyers, 461 F. Supp. 2d at 693.

statute must be read in their context and with a view to their place in the overall statutory scheme."[109] Bearing this in mind, "Section 230(c)(1) does not bar 'any cause of action,' as *Zeran* holds and as Craigslist contends, but instead is more limited—it bars those causes of action that would require treating an [internet company] as a *publisher* of third-party content," as its title and caption indicated.[110] "First and foremost," the court explained, "*Zeran* overstates the 'plain language' of Section 230(c)(1)."[111] The subsection's text never mentioned "immunity."[112] And the *Zeran* court had itself indicated, before phrasing its holding in sweeping language, that the provision was limited to torts based on a provider's publisher-like exercise of traditional editorial functions.[113] Subsequent courts granting broad immunity reasoned based on *Zeran*'s interpretation, not § 230(c)(1)'s text, it noted.[114] Moreover, the broad immunity approach gave companies no incentive to filter content, because they would be protected whether they did or didn't police content and filtering would cost more than not filtering.[115] So doing, the *Zeran* interpretation undercut the CDA's second purpose—protecting users.[116]

Rejecting *Zeran*'s approach, the district court held that Section 230(c)(1) "does not grant immunity per se [but] does prohibit treatment as a publisher, which, quite plainly, would bar any cause of action that requires, to establish liability, a finding that [the company] published third-party content."[117] Because the FHA provision at issue made it illegal "[t]o make, print, *or publish* . . . any [discriminatory] notice, statement, or advertisement," § 230(c)(1) did in fact apply and Craigslist could not be held liable as a publisher of the discriminatory

---

[109] *Id.* at 693.
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.* at 688–89 (quoting Zeran, 129 F.3d at 330) ("Specifically, § 230 precludes . . . lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content.").
[114] Chicago Lawyers, 461 F. Supp. 2d at 688–89; *but see* Barnes, 570 F.3d at 1100 (noting that the Ninth Circuit's decisions in Roommates, 521 F.3d at 1171 (9th Cir. 2008), and *Barnes* rested not on "broad statements of immunity" but on "careful exegesis").
[115] Chicago Lawyers, 461 F. Supp. 2d at 691.
[116] *See id.*
[117] *Id.* at 696.

housing ads.[118] The Seventh Circuit affirmed this result and the court's definitional approach.[119]

Notwithstanding most circuits' adoption of the immunity approach, the Court should resolve this circuit split by adopting the Seventh Circuit's definitional interpretation of § 230(c)(1), which is the more faithful reading of this provision.[120] As the persistent existence of this circuit split shows, the language of § 230(c)(1) is not plain but ambiguous.[121] Therefore, the Court should consider the text *in context*.[122] While powerful online communication companies no doubt prefer the majority approach (and could lobby for a statute that grants such broad immunity), the Seventh Circuit's definitional approach is the better reading for three reasons. First, the text of § 230(c)(1) does not grant "immunity"—either broad or narrow.[123] Second, the definitional approach functionally aligns § 230(c)(1) with § 230(c)(2) and accords with § 230(c)(1)'s title and caption.[124] And third, the definitional approach more closely tracks Congress' *two* stated purposes for § 230.[125]

First, as the Seventh Circuit noted in *Chicago Lawyers,* the majority's immunity approach grows out of an erroneous and overbroad reading of § 230 established in *Zeran*.[126] *Zeran* claimed that § 230, "[b]y its plain language . . . creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[127] But as the Seventh Circuit points out, § 230(c)(1) does not use the word "immunity" or words like "shall not be held liable for" that are

---

[118] *Id.* at 696–98.
[119] *Id.* at 667.
[120] The Ninth Circuit, while still using an immunity approach, narrowed its approach after *Roommates.com* and has adopted some of the language of the Seventh Circuit's definitional approach. *See* Barnes, 570 F.3d at 1100.
[121] *See* Graham City Soil & Water Conservation Dist. v. United States. ex rel. Wilson, 125 S. Ct. 2444, 2451 n.2 (2005) (declaring a statute ambiguous "because its text, literally read, admits of two plausible interpretations").
[122] *See* Yates v. United States, 574 U.S. 528, 539–40 (2015).
[123] *See* 47 U.S.C. § 230(c)(1); *see also* Chicago Lawyers, 461 F. Supp. 2d at 693 (§ 230(c)(1) "does not mention 'immunity' or any similar term or phrase . . . [unlike § 230(c)(2)] which uses language that unequivocally creates immunity: 'no provider or user of an interactive computer service *shall be held liable* on account of . . .'").
[124] *See* 47 U.S.C. § 230(c)(2); City of Chicago, Ill. v. StubHub!, Inc., 624 F.3d 363, 365 (7th Cir. 2010).
[125] *See supra* notes 60–62 and accompanying text.
[126] Chicago Lawyers, 461 F. Supp. 2d at 693.
[127] Zeran, F.3d at 330.

commonly understood to grant immunity.[128] Section 230(c)(2), by contrast, does use traditional immunity-granting words, reading "no [provider]. . . shall be held liable on account of."[129] As the Court has noted, "where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[130] So, if Congress intended § 230(c)(1) to grant broad immunity in the manner of (c)(2), it likely would have used the same or similar words in each subsection.

Second, as the Seventh Circuit emphasized in another case, *City of Chicago v. StubHub!*, the definitional approach, unlike the broad immunity approach, properly considers the provision's full, contextualized purpose, as shown by its title and caption.[131] The Supreme Court understands that, "[a]lthough section headings cannot limit the plain meaning of a statutory text, they supply cues as to what Congress intended."[132] Section 230 is titled "Protection for private blocking and screening of offensive material."[133] Subsection (c) is captioned "Protection for 'Good Samaritan' blocking and screening of offensive material."[134] Because both headings reference "offensive material," this strongly suggests they were intended to limit defamation-type, content-based claims, not *all* tort claims as the broad immunity approach holds. [135]

StubHub! drives home the vast over-applicability of the broad immunity approach. In *StubHub!*, an online ticket marketplace, StubHub!, claimed that § 230(c)(1) exempted it from having to collect and remit an amusement tax imposed by Chicago.[136] StubHub! claimed that under § 230's broad immunity it was exempted from collecting taxes on the ticket transactions it facilitated.[137] Rejecting this interpretation, Judge Easterbrook noted that "Section 230's title, 'Protection for private blocking and screening of offensive material', does not suggest that it limits taxes that have nothing to do with

---

[128] *See* 47 U.S.C. § 230(c)(1); *see* Chicago Lawyers, 461 F. Supp. 2d at 693.
[129] *See* 47 U.S.C. § 230(c)(2); *see* Chicago Lawyers, 461 F. Supp. 2d at 693.
[130] Russello v. United States, 104 S. Ct. 296, 300 (1983).
[131] StubHub!, Inc., 624 F.3d at 365.
[132] Merit Mgmt. Grp., LP v. FTI Consulting, Inc., 138 S. Ct. 883, 893 (2018); *cf.* Yates v. United States, 574 U.S. 528, 539 (2015).
[133] 47 U.S.C. § 230.
[134] 47 U.S.C. § 230(c).
[135] As the legislative history of the CDA shows, the "offensive material" Congress was concerned with was online pornography, defamation, harassment, and disparagement. *See supra* notes 58–64, 66.
[136] StubHub!, 624 F.3d at 365.
[137] *See id.*

[offensive content].”[138] Nor, he said, did “Subsection (c)'s caption, ‘Protection for ‘Good Samaritan’ blocking and screening of offensive material[.]’”[139] Both the title and caption instead suggested Congress intended § 230(c)(1) to apply to publication-based claims like the disparagement and defamation claims at issue in *Stratton Oakmont* and *Cubby*.[140] *Zeran*’s approach, he emphasized, potentially reaching even tax claims, far exceeded Congressional intent for § 230.[141] And, as the district court had noted in *Chicago Lawyers*, the *Zeran* approach undermined the user protections Congress had intended to encourage, by eliminating financial incentive for companies to police their own content.[142]

The narrow immunity approach addresses this latter concern by limiting immunity to cases involving the company’s engagement in traditional publisher-type activities like editing and promoting/removing material. But only the definitional approach hews to the text of § 230(c)(1) by not granting “immunity” Congress did not authorize. For this reason, even though the majority of circuits currently do otherwise, the Court should adopt a definitional approach to § 230(c)(1) and reject both the broad and narrow immunity approaches.

C. Reconsidering whether § 230(c)(1) bars the Force plaintiffs’ algorithmic material support claims

Of course, the *Force* plaintiffs did not seek cert merely to resolve this circuit split. They hoped for a finding that § 230(c)(1) does not bar material support claims based on Facebook’s friend suggestion algorithm.

Under the Seventh Circuit’s definitional approach, these claims are not barred.[143] The *Force* plaintiffs asserted claims based on three provisions of the Anti-Terrorism Act (ATA): 18 U.S.C. §

---

[138] *Id.*
[139] *Id.*
[140] *See id.* at 365–66; *see* 141 CONG. REC. H8469-70 (daily ed. Aug. 4, 1995) (Remarks of Rep. Cox, comparing Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995) with Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991)).
[141] *Cf.* StubHub!, 624 F.3d at 366, *with* Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997).
[142] Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 681, 693 (N.D. Ill. 2006), *aff’d sub nom.* 519 F.3d 666 (7th Cir. 2008).
[143] *See* StubHub!, 624 F.3d at 366.

2333(a), § 2339A, and § 2339B.[144] Unlike a defamation claim or the FHA claims at issue in *Chicago Lawyers*, liability under these provisions does not depend on whether Facebook is a publisher.[145] Rather, "any person" (natural or corporate) who knowingly provides "material support or resources" to a prohibited person or organization is potentially liable.[146]

The *Force* plaintiffs might also prevail if the Court adopts an immunity approach, under possible reasonings offered by Chief Judge Katzmann in his *Force* dissent.[147] As the dissent notes, Facebook's friend suggestion algorithm is arguably not "content provided by another internet content provider."[148] If that is so, the algorithm-based claims are not exempted under either the broad or narrow immunity approach. Alternatively, Facebook's friend suggestion algorithm may not perform a traditional "publishing" function, so under the narrow immunity approach the claims are not barred.[149]

As Judge Katzmann first suggests, Facebook's friend suggestions are not "information provided by another information content provider" and are thus completely outside § 230(c)'s scope.[150] The algorithms allegedly create new informational content from raw data about user activities.[151] The *Force* majority rejected this view, using a "material contribution" test developed for defamation cases.[152] Under that test, because Facebook did not "directly and materially contribute to what made the content itself *unlawful*," Facebook did not "develop" the content. It merely chose where to "present" Hamas' content.[153] Like a traditional editor making decisions about what to feature on the front page and what to bury inside, Facebook's friend algorithm merely identified some profiles to place more prominently than the rest.[154]

---

[144] *See* Force, 934 F.3d at 61 n.10. Plaintiffs bringing civil claims under § 2333 on a secondary liability material support theory must first step into the shoes of a prosecutor and show a violation of § 2339A or § 2339B, which violation serves as the basis of civil liability. *See supra*, note 21.
[145] *See* Chicago Lawyers, 461 F. Supp. 2d at 693.
[146] *See* 18 U.S.C. §§ 2339A, 2339B (both providing that "whoever" provides material support as defined by the statute shall be punished under the statute).
[147] *See* Force, 934 F.3d at 77 (Katzman, C.J. concurring in part and dissenting in part).
[148] *See* 47 U.S.C. § 230(c)(1); *see* Force, 934 F.3d at 77.
[149] Force, 934 F.3d at 77.
[150] *See* 47 U.S.C. § 230(c)(1).
[151] *See* Force, 934 F.3d at 77.
[152] *See id.* at 68–70.
[153] *See id.* at 68–69.
[154] *See id.* at 66–67.

But as the dissent rightly points out, if Facebook's algorithm operates as the plaintiffs claim, it does not just present friend suggestions but *creates* these suggestions.[155] Put another way, Facebook's algorithm is not like Buzzfeed or another site that skims your blog posts and arranges completed content you posted elsewhere. It is like a researcher who pokes through your trashcan to uncover secret habits and patterns about your life—patterns you have not knowingly revealed and may not have yourself recognized—analyzes the resulting data, and sells your name in a database to purveyors of items your trash reveals you might want to purchase. Your *trash* isn't the product this garbage-picking researcher is selling. And the database he has produced is not an altered or edited version of your trash. Its value lies in the synthesized product—new *information* which the researcher, not you, created. As this analogy shows, the *Force* dissent's interpretation is correct. Facebook's algorithms are content created by Facebook, not another user.[156] Section 230 should be "irrelevant" to these claims.[157]

As Judge Katzmann alternatively suggests, Facebook's friend suggestion algorithm is outside the traditional understanding of what it means to "publish" another's content.[158] Section 230, he explains, "does not apply whenever a claim would treat the defendant as 'a publisher' in the abstract, immunizing defendants from liability stemming from any activity in which one thinks publishing companies commonly engage."[159] It applies when the service acts as "*the* publisher" of the specific content at issue by engaging in editorial functions like "deciding whether to publish, withdraw, postpone, or alter content" submitted by another.[160] That is not the case with Facebook's algorithm. To illustrate, imagine you are a published book author. Amazon, having tracked a customer's past purchases, determines that customer would enjoy your latest book. It suggests the customer buy your book. Amazon, of course, is not the publisher or editor of your book. It's making a sales connection. Following this logic, Facebook is not immune for suits based on an algorithm that performs not editorial but *sales* type functions.[161]

---

[155] *See id.* at 77 (Katzmann, C.J., concurring in part and dissenting in part).
[156] *See id.* at 82 (J. Katzmann, dissenting in part).
[157] *See* City of Chicago, Ill. v. StubHub!, Inc., 624 F.3d 363, 366 (7th Cir. 2010).
[158] *See* Force, 934 F.3d at 81 (J. Katzmann, dissenting in part).
[159] *See id.* at 80–81.
[160] *Id.* at 81.
[161] *See id.* at 82.

D. The ATA's proximate causation requirement is the appropriate statutory hurdle by which to screen algorithmic material support claims

Section 230 is not the only statutory hurdle lying between plaintiffs and recovery. The ATA itself presents a formidable hurdle for plaintiffs attempting to bring algorithmic material support claims against social media companies like Facebook.[162]

The ATA's private right of action is available to a United States national who has been injured "by reason of an act of international terrorism."[163] "By reason of" equates to proximate cause.[164] Courts that have considered the ATA's proximate causation requirement in material support claims have required "some direct relation between the injury asserted and the injurious conduct alleged."[165] While the directness of the relationship is only one aspect of a proximate cause analysis, it is a key requirement.[166] A "tenuous" connection between the social media company's algorithmic conduct and the terrorist act does not suffice.[167]

Though no court has yet considered this issue, it will be very difficult for plaintiffs bringing algorithmic social media material support claims to meet this proximate cause standard.[168] To survive dismissal for failure to state a claim under the ATA, a plaintiff would likely have to show that the algorithm-generated friend suggestion directly caused the terrorist actor to connect with a listed terrorist group *and* that the resulting online interaction proximately led to the specific action that injured the plaintiff.[169] Most algorithmic material support cases would be unable to meet this standard, given the huge number of possible influences on any given terrorist actor and the minor weight of a single friend suggestion. Social media companies therefore need not fear wide exposure to expensive and intrusive discovery proceedings for material support claims not barred by Section 230.

It is fair to social media companies that an algorithmic material support claim should have to clear the ATA's significant proximate causation hurdle. But fairness also requires that victims of terror attacks

---

[162] *See* Retana v. Twitter, Inc., 419 F. Supp. 3d 989, 995 (N.D. Tex. 2019).
[163] 18 U.S.C. § 2333(a).
[164] *See* Retana, 419 F. Supp. 3d at 995.
[165] Crosby v. Twitter, Inc., 921 F.3d 617, 624 (6th Cir. 2019) (quoting Bridge v. Phoenix Bond & Indem. Co., 553 U.S. 639, 654 (2008)); Retana, 419 F. Supp. 3d at 995.
[166] *See* Crosby, 921 F.3d at 624.
[167] *See id*.
[168] *Cf.* Crosby, 921 F.3d at 624 *with* Retana, 419 F. Supp. 3d at 995.
[169] *Cf.* Crosby, 921 F.3d at 624 *with* Retana, 419 F. Supp. 3d at 995.

pleading plausible material support claims against social media companies should not find those claims barred by the CDA. The ATA, not Section 230, is the appropriate statutory hurdle by which to screen out tenuous algorithmic material support claims.

In conclusion, if the Court in future resolves the current circuit split by adopting the Seventh Circuit's definitional approach, algorithmic material support claims like those brought by the *Force* plaintiffs would not be barred by § 230(c)(1). Or, the Court could adopt an immunity approach and accept one of Judge Katzmann's arguments that the friend suggestion algorithm-based claims are not barred. Or finally, Congress could amend Section 230 to create a "carve-out" for terrorism claims, as has recently been proposed.[170] Should any of these happen in a case where the plaintiffs can show proximate cause, lower courts must next determine whether the material support statute's civil liability provision, as applied to Facebook's friend suggestion algorithm, is constitutional. Assuming for argument's sake algorithmic material support claims might someday pass the statutory hurdles posed by the CDA and the ATA, this article next analyzes the constitutional hurdle posed by the First Amendment.

II. THE CONSTITUTIONAL HURDLE: POTENTIAL FIRST AMENDMENT LIMITS ON MATERIAL SUPPORT LIABILITY BASED ON FACEBOOK'S FRIEND SUGGESTION ALGORITHM

If the Supreme Court holds or Congress declares that Section 230 does not bar claims based on Facebook's algorithmic friend suggestions, plaintiffs like those in *Force* will next face a constitutional hurdle. Facebook will argue that its algorithm is constitutionally protected speech that the government seeks to impermissibly regulate. It will challenge the constitutionality of 18 U.S.C. §§ 2339A, 2339B, and 2333 as applied to this algorithm. This section considers these hypothetical arguments and finds them convincing.

The First Amendment provides in relevant part that "Congress shall make no law . . . abridging the freedom of speech."[171] The "freedom of speech" thus guaranteed by the Constitution is expansive.[172] It embraces discussion of "all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period."[173] In order to adequately protect valuable speech (and avoid the danger of allowing government to decide speech's value) the Court has held that the First Amendment

---

[170] *See infra* Section II.
[171] U.S. CONST. amend. I, cl. 3.
[172] *See, e.g.*, Roth v. United States, 354 U.S. 476, 492 (1957).
[173] *Id.* at 488.

protects such diverse "speech" as advertising, flag burning, video games, and data mining.[174]

But the freedom of speech, while fundamental, is not absolute.[175] Most speech is protected from abridgment, but "[t]here are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem."[176] These include incitement, true threats, obscenity, and "fighting words."[177] And even speech protected under the First Amendment may be regulated, under limited circumstances.[178] Different kinds of speech restrictions trigger differing levels of scrutiny: content-based regulations and regulations of political speech receive strict scrutiny, while commercial speech regulations, for example, receive less rigorous scrutiny.[179]

Thus, a court considering whether claims like the ones in *Force* clear the constitutional hurdle must resolve three questions. First, is Facebook's friend suggestion algorithm "speech"? Second, assuming Facebook's algorithm is indeed speech, what level of protection, if any, does the First Amendment provide it? And third, do §§ 2339A, 2339B, and 2333 permissibly regulate this "algorithmic speech"? This section addresses each of these questions, in turn.

A. Is Facebook's friend suggestion algorithm "speech"?

Both "the creation and dissemination of information are speech within the meaning of the First Amendment."[180] But applying this definition to information that is created and disseminated by machines rather than humans, at least in part, raises tricky questions about speech limits. As one scholar has noted, giving "[t]oo little protection [to machine-generated or machine-facilitated speech] would disserve speakers who have evolved beyond the printed pamphlet . . . [while] [t]oo much protection would threaten to constitutionalize many areas

---

[174] *See, e.g.*, 44 Liquormart, Inc., v. Rhode Island, 517 U.S. 484 (1996) (liquor price advertising); Texas v. Johnson, 491 U.S. 397, 417 (1989) (flag burning); Brown v. Entm't Merchs. Ass'n, 564 U.S. 786 (2011) (graphically violent video games); Sorrell v. IMS Health Inc., 564 U.S. 552 (2011) (data mining).
[175] *See* Chaplinsky v. State of New Hampshire, 315 U.S. 568, 571–72 (1942).
[176] *Id.*; Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (incitement); Watts v. United States, 394 U.S. 705, 707 (1969) (true threats).
[177] Cohen v. California, 403 U.S. 15, 19–20 (1971).
[178] *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 28 (2010).
[179] *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010) (strict scrutiny); Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 475 (1989) (lesser scrutiny for commercial speech).
[180] Sorrell, 564 U.S. at 570.

of commerce and private concern without promoting the values of the First Amendment."[181]

First Amendment scholar Stuart Minor Benjamin argues that algorithmic selection and promotion of specific content tailored to specific users is speech under Supreme Court precedent.[182] Benjamin identifies "two—and only two—elements for First Amendment coverage" of digital speech.[183] First, that the communications platform's "programmers or operators either create programming or choose what to air."[184] And second, "that in doing so they seek to communicate messages on a variety of topics."[185] The Supreme Court broadly interprets the "message" requirement and has stated that "a narrow, succinctly articulable message is not a condition of constitutional protection."[186]

While the precise nature of Facebook's algorithms is a closely guarded trade secret, public information shows some of the company's algorithms likely satisfy both elements of Benjamin's algorithmic speech test.[187] For example, in early 2018, Facebook CEO Mark Zuckerberg announced a change to Facebook's algorithms. Zuckerberg said he was "changing the goal I give our product teams from focusing on helping you find relevant content to helping you have more meaningful social interactions."[188] Facebook would now program its algorithms to "prioritize posts that spark conversations and meaningful interactions between people," and "show these posts higher in [the user's] feed." [189] Prioritized posts would be those "that inspire back-and-forth discussion in the comments [and those] you might want to share and react to."[190]

---

[181] Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1498 (2013).
[182] Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445, 1447 (2013) [hereinafter Benjamin, *Algorithms*]; *see also* Stuart Minor Benjamin, *Transmitting, Editing, and Communicating: Determining What "The Freedom of Speech" Encompasses*, 60 DUKE L.J. 1673, 1695 (2011).
[183] Benjamin, *supra* note 182, at 1460.
[184] *Id.*
[185] *Id.*
[186] Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston, 515 U.S. 557, 569 (1995).
[187] Corporations like Facebook are speakers fully protected by the First Amendment. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 342 (2010).
[188] Adam Mosseri, *Bringing People Closer Together*, FACEBOOK BLOG (January 11, 2018, 4:28 PM), https://about.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/.
[189] *Id.*
[190] *Id.*

These public statements indicate the company's algorithms are likely to be speech, for two reasons. First, "inspiring back-and-forth discussion" is at the heart of the marketplace of ideas and self-governance theories that guide First Amendment jurisprudence.[191] Next, they show that Facebook's newsfeed algorithms are selective, satisfying the "choose what to air" prong of the first element of Benjamin's speech test. The algorithms analyze user data and, based on criteria set by Mark Zuckerberg and implemented by Facebook engineers, select which posts a user will see and in what order.[192] The algorithms also reflect and communicate a pro-community and social engagement message, satisfying the test's second element.

Benjamin compares this kind of algorithm to a person who selects certain news clippings to post on a physical bulletin board.[193] Because the bulletin board reflects its creator's substantive point of view, it is speech.[194] Transferring the bulletin board to the internet and automating the selection doesn't change the analysis, because these steps change "nothing relevant to free speech coverage under the Supreme Court's jurisprudence."[195] Here, because Zuckerberg's personal decisions to promote or suppress certain content would be protected under the First Amendment, Facebook's algorithms retain that protection.[196]

Admittedly, less is known about Facebook's friend suggestion algorithm (at issue in *Force*) than about the newsfeed algorithm discussed above.[197] It's possible that the friend suggestion algorithm,

---

[191] *See* Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J. concurring), overruled in part by Brandenburg v. Ohio, 395 U.S. 444 (1969).

[192] As noted above, this article assumes for the sake of argument that the friend suggestion algorithm operates as alleged by the plaintiffs in *Force*. *See supra*, note 18. This subsection's analysis further assumes for the sake of argument that Zuckerberg directs programming goals for the friend suggestion algorithm as for the newsfeed algorithm. *See supra*, notes 188–190 and accompanying text.

[193] *See* Benjamin, *supra* note 182, at 1465.

[194] *See* Hurley, 515 U.S. at 569.

[195] *See* Benjamin, *supra* note 182, at 1465.

[196] *See* Emily Stewart, *Mark Zuckerberg is Essentially Untouchable at Facebook*, VOX, (Dec 19, 2018, 11:19 AM), https://www.vox.com/technology/2018/11/19/18099011/mark-zuckerberg-facebook-stock-nyt-wsj (Mark Zuckerberg owns 60% of Facebook's voting shares, which makes his decisions there essentially uncheckable).

[197] *See* Amelia Tait, *Why does Facebook Recommend Friends I've Never Met?*, WIRED, (May 29, 2019), https://www.wired.co.uk/article/facebook-people-you-may-know-friend-suggestions; *but see*, *Where do People You may*

unlike the newsfeed ranking algorithm, might have no basis in Facebook's point of view. It could suggest friends based on non-ideological factors like geolocation data. If so, the friend suggestion algorithm might be regulable commercial conduct, not protected speech.[198] But if, as the *Force* plaintiffs allege, the algorithm identifies potential Hamas recruits based on shared interests and creates new friend suggestions based on that information, the friend suggestion algorithm satisfies Benjamin's test. The friend suggestion algorithm "create[s] content" and "select[s] content to present" by taking raw data about what users are *interested in* and generating a friend suggestion consisting of a line of text, picture, and link.[199] It selects and promotes these suggestions to maximize communicative impact. By these actions, Facebook communicates a message that more social connection is desirable. Facebook's friend suggestion algorithm thus passes Benjamin's test for algorithmic "speech."

B. Is algorithmic speech fully protected under the First Amendment?

Assuming, then, that Facebook's algorithm is speech, is it protected by the First Amendment? As discussed above, the Supreme Court has expansively defined protected speech. Only a few historically bounded categories of speech, like incitement, true threats, obscenity, and fighting words, are outside the Amendment's protection.[200] While some speech posted by Hamas on Facebook may be incitement or true threats, Facebook's friend suggestion algorithm's

---

Know Suggestions Come From on Facebook?, FACEBOOK https://www.facebook.com/help/163810437015615 (listing factors Facebook uses to generate these suggestions).

[198] An example of a commercial conduct algorithm is Amazon's product suggestions. It can be hard for courts to draw the line between regulable conduct and speech protected by the First Amendment. *Cf.* Dana's R.R. Supply v. Attorney Gen., Fla., 807 F.3d 1235, 1248 (11th Cir. 2015) (Florida's anti-surcharge law was an impermissible speech regulation) *with* Rowell v. Pettijohn, 816 F.3d 73, 80 (5th Cir. 2016), *cert. granted, judgment vacated*, 137 S. Ct. 1431 (2017) (Texas' anti-surcharge law was a conduct regulation only incidentally implicating speech). The Supreme Court resolved this circuit split in favor of speech. The difference between a conduct regulation and a speech regulation is whether they promote communication (Facebook) or commerce (Amazon).

[199] *See* Benjamin, *supra* note 182, at 1460.

[200] *See* Cohen v. California, 403 U.S. 15, 19–20 (1971).

output is certainly not.[201] Facebook's friend suggestion algorithm falls into no First Amendment exemption. So, it is protected.[202]

Next, it's possible that Facebook's algorithm might be "commercial speech." If so, it would receive second class First Amendment protection.[203] The outer boundaries of commercial speech are not firmly established. Core commercial speech "does no more than propose a commercial transaction."[204] But speech that mixes pure commercial elements like price advertising with non-commercial elements like education or editorial material may also be commercial speech.[205] In determining whether speech is commercial, the Supreme Court has considered the function and motivation of the speech as a whole. If the speaker's motivation is largely economic, then that speech may be less easily chilled and may therefore need less First Amendment protection.[206]

Where Facebook's friend suggestion algorithm would land in this analysis is a bit unclear. No court has yet decided the issue of whether these kinds of algorithms are speech, much less whether such algorithms might be entitled to less protection.[207] Facebook is free for users, so its friend suggestions aren't proposing a classic paid transaction. The suggestions are not exactly ads for any product or service provided by Facebook. And the suggestions are strongly related to promoting conversation and connection, which are issues of public concern at the core of First Amendment rationales. All of these factors weigh in favor of full protection for this algorithmic speech. On the other hand, Facebook's friend suggestions do arguably propose a commercial transaction central to the social media business model—that one user "friend" another, on a platform where increased

---

[201] *See* Brandenburg v. Ohio, 395 U.S. 444, 47 (1969) (per curiam).
[202] *See, e.g.*, Cohen, 403 U.S. at 19.
[203] *See* Bd. of Trs. of State Univ. of N. Y. v. Fox, 492 U.S. 469, 475 (1989) (commercial speech regulation must be justified by a "substantial interest;" the regulatory means chosen need not be the least restrictive available).
[204] *See* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976).
[205] *See* Bolger v. Youngs Drug Prod. Corp., 463 U.S. 60, 66 (1983) (holding that pamphlets which included both general information about contraceptives and specific information encouraging customers to purchase them from defendant's drug store were commercial speech).
[206] *See* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 772 (1976) (citing the greater hardiness of commercial speech as a rationale for its lower level of protection).
[207] *But see* Jian Zhang v. Baidu.com Inc., 10 F. Supp. 3d 433, 440 (S.D.N.Y. 2014) (holding that censorship algorithm that removed certain search results was fully protected speech).

connection and engagement means more time spent scrolling and increased ad revenue. Facebook's motivation for urging these connections is certainly economic at base. And arguably, there is no risk of chilling an algorithm, as it cannot deviate from its programming.[208]

Further speculation on this fascinating subject is outside the scope of this article, but the trend of recent Supreme Court precedent is to declare speech "commercial" only when it *merely* proposes a commercial transaction.[209] For this reason alone, it's highly likely that Facebook's algorithmic speech would receive full, non-commercial protection, as it also communicates a pro-social message. Assuming therefore that this speech would receive full protection under the First Amendment, the next section considers constitutional limitations on the algorithmic material support claims.

C. Does the ATA's material-support prohibition violate the First Amendment as applied to Facebook's friend suggestion algorithm?

Assuming that Facebook's friend suggestion algorithm is fully protected speech, the next relevant question is whether the First Amendment limits the government's ability to hold Facebook liable for that speech under three provisions of the Anti-Terrorism Act: §§ 2339A, 2339B, and 2333.[210] Section 2333 provides a civil cause of action to people injured by international terrorist acts. Sections 2339A and B criminalize providing material support or resources to terrorists and designated foreign terrorist groups. These provisions are not, on their face, speech regulations. But, as applied to Facebook's algorithm, the regulations trigger the First Amendment, because where the only "conduct" the State seeks to punish "is the fact of communication" the regulation is one of speech, not of conduct.[211] Furthermore, because these provisions bar only speech that materially supports terrorists (and not speech that, for example, hinders terrorists), they are "content-

---

[208] *See* Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1499 (2013).

[209] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011) ("While the burdened speech results from an economic motive, so too does a great deal of vital expression.").

[210] As discussed previously, plaintiffs bringing secondary-liability material support claims under § 2333 must prove a violation under § 2339A or B. *See supra* note 21.

[211] *See* Cohen, 403 U.S. at 18.

based" speech regulation.[212] Such restrictions receive strict scrutiny.[213] Strict scrutiny demands a compelling government interest and that the challenged regulation is the most narrowly tailed means of achieving that end.[214]

The Supreme Court considered an as-applied First Amendment challenge to § 2339B in *Holder v. Humanitarian Law Project*.[215] *Holder* involved U.S. citizens who "wished to provide support for the political and humanitarian activities" of two groups, the Kurdistan Workers' Party (PKK) and the Liberation Tigers of Tamil Eelam (LTTE).[216] Both organizations had been designated by the U.S. Secretary of State as "foreign terrorist organizations."[217] The plaintiffs wished to support the organizations' lawful activities by providing "legal training, and political advocacy."[218] Because § 2339B criminalized providing such support, they could not. The plaintiffs sued claiming that § 2339B violated their First Amendment freedom of speech by "criminaliz[ing this speech] without requiring the Government to prove that plaintiffs had a specific intent to further the unlawful ends of those organizations."[219]

The *Holder* Court rejected the government's arguments that the material support ban regulated only non-expressive conduct or that it was a conduct regulation that imposed only incidental burdens on speech.[220] As applied to the plaintiffs, the law banned communications—training and advocacy—in support of the PKK and LTTE, acting as a content-based speech restriction. The Court therefore employed "rigorous" scrutiny.[221] First, the government interest asserted—preventing terrorist attacks—was compelling and "an urgent

---

[212] *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 28 (2010).
[213] *See, e.g.*, United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 804 (2000).
[214] *Id.*
[215] *Holder*, 561 U.S. at 28.
[216] *Id.* at 9–10.
[217] *Id.* at 9.
[218] *Id.*
[219] *Id.* at 37.
[220] Holder, 561 U.S. at 27–8.
[221] *Id.*; *see also* Williams-Yulee v. Fla. Bar, 575 U.S. 433, 444 (2015) (Roberts, J.) (describing *Holder* as a strict scrutiny class); *but see* Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 672–73 (describing the Court's characterization of *Holder* as a strict scrutiny case as "lawyerly sleight of hand").

objective of the highest order."[222] The Court next considered whether the statute needlessly prohibited speech-based support intended to support the organizations' peaceful activities.[223] In a departure from ordinary strict scrutiny analysis, the Court deferred to Congress' determination that a ban on speech-based support to the group was necessary.[224] Given the structural realities of terrorist groups like these, plaintiffs' direct support for peaceful activities indirectly supports the groups' violent activities. Support, the Court emphasized, was fungible.[225] Given the government's exceedingly strong interest in preventing terror attacks and the special competency of the political branches in evaluating the risks involved, § 2339B as applied was sufficiently narrow.[226]

However, the *Holder* Court emphasized, its decision did not mean "any future applications of the material-support statute to speech . . . [would] survive First Amendment scrutiny."[227] "In particular," the Court stated, "we in no way suggest that a regulation of *independent* speech would pass constitutional muster, even if the Government [shows] that such speech benefits foreign terrorist organizations."[228] This caveat is particularly relevant to the claims raised in *Force*. First, the government's interest in allowing civil suits is less compelling than its interest in preventing terror attacks. Second, as applied to independent speech like Facebook's, the statute is not a sufficiently tailored means of achieving this interest.

In the "compelling government interest" prong of the strict scrutiny analysis, the *Force* claims might survive but carry less weight than the interest asserted in *Holder*. The *Holder* court noted that the government's interest in preventing acts of terrorism was "an urgent objective of the highest order."[229] And, in *Holder*, the government was directly asserting that interest through § 2339B.[230] In *Force*, the plaintiffs asserted §§ 2339A and B *through* § 2333, the civil liability provision.[231] The government's regulatory interest in *Force*, therefore,

---

[222] Holder, 561 U.S. at 28; *see* Tsesis, *supra* note 221, at 672–73 (arguing that the *Holder* Court approved less narrow means to balance the super-compelling interests of national security and prevention of terrorist attacks).
[223] *See* Holder, 561 U.S. at 29–39.
[224] *See id.* at 34–35.
[225] *Id.* at 37.
[226] *Id.* at 36.
[227] *Id.* at 39.
[228] *See id.* at 39 (emphasis added).
[229] Holder, 561 U.S. at 28.
[230] *Id.* at 11.
[231] *See* Force v. Facebook, Inc., 934 F.3d 53, 61 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020).

isn't prevention of terrorist acts, but enabling victims of such attacks to find justice. This is probably less compelling than preventing the attacks themselves.

In the "narrowly tailored means" prong of the strict scrutiny analysis, the ATA's material support provisions, as applied to the *Force* plaintiffs' claims, are unlikely to survive. Facebook's algorithm is *independent* speech, a restriction of which the *Holder* Court stated was undecided by that opinion and indicated was unlikely to succeed.[232] The *Holder* plaintiffs wanted to work directly with the PKK and LTTE, training members and advocating on the organization's behalf.[233] Facebook, in contrast, is not working with Hamas. It deploys its algorithm to increase use of and engagement with its site. Support of Hamas is secondary and unintentional.[234] If the material support statute can criminalize such speech, it is dangerously broad.[235]

Of course, there is a legitimate argument for why prohibiting civil suits based on independent speech that has the effect of providing material support is the most narrowly tailored means available. Facebook is arguably a uniquely powerful market force, so its friend suggestions may be uniquely effective at providing recruits. Given this, civil liability might be a necessary means of forcing Facebook to address the problem, given the government's limited means to do so and Facebook's significant ones. However, this argument will fail. When national security is at issue, courts are especially reluctant to allow suits that might undercut the effectiveness of executive enforcement.[236] The government may prefer to shield Facebook from liability if terrorist groups that communicate via American technology platforms are easier for U.S. intelligence to monitor. Furthermore, under strict scrutiny the *most* narrowly tailored means to achieve the government's interest is required. A statute providing that Facebook may be held liable only for material support it intentionally or directly provides to Hamas (as, say, a contractor) would be more narrowly tailored. Unless the Court finds that Congress had no narrower means of effectively preventing a service like Facebook from providing material support through its friend suggestion algorithm, the statute

---

[232] *Id.* at 39 ("In particular, we in no way suggest that a regulation of independent speech would pass constitutional muster, even if the Government were to show that such speech benefits foreign terrorist organizations.").
[233] *See id.* at 36.
[234] Once Facebook is made aware of its speech's effect, it may knowingly or recklessly allow it to continue. But this would still be a lower level of *mens rea* than the "intentional" training and advocacy support approved in *Holder*.
[235] *See id*. at 31–32.
[236] *See* Trump v. Hawaii, 138 S. Ct. 2392, 2409 (2018); Korematsu v. United States, 323 U.S. 214, 220 (1944).

will not survive means analysis. Considering the *Holder* Court's concern about allowing Congress to create unbounded liability for independent speech that provides support to terrorist organizations, § 2333 thus applied would be struck down as an impermissible regulation of Facebook's algorithmic speech.

CONCLUSION

Algorithmic material support claims like those brought in *Force* are long shots. As currently written and interpreted by a majority of courts, § 230(c)(1) provides potent immunity from such claims. However, given recent calls to reform Section 230, it is possible that this statutory hurdle may be lowered—or removed entirely.[237] Congress has begun considering proposals to reform Section 230.[238]

---

[237] *See, e.g.*, Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (May 28, 2020) (directing federal agencies to interpret § 230(c) "narrowly" and "[t]he Attorney General [to] develop a proposal for Federal legislation that would be useful to promote the policy objectives of this order"). This executive order and much of the recent clamor for reform of § 230(c) was driven largely by President Trump's frustration with Twitter, which in May 2020, began adding labels contextualizing the President's most false and inflammatory tweets. *See id.* ("Twitter now selectively decides to place a warning label on certain tweets in a manner that clearly reflects political bias. As has been reported, Twitter seems never to have placed such a label on another politician's tweet. As recently as last week, Representative Adam Schiff was continuing to mislead his followers by peddling the long-disproved Russian Collusion Hoax, and Twitter did not flag those tweets. Unsurprisingly, its officer in charge of so-called 'Site Integrity' has flaunted his political bias in his own tweets."); *see also* Kate Conger, *Another Tweet from Trump Gets a Label from Twitter*, N.Y. TIMES, (June 23, 2020), https://www.nytimes.com/2020/06/23/technology/trump-twitter-label-seattle.html. However, concerns about § 230(c) and its expansive interpretation, and calls for Congress to reconsider its provisions, long pre-date the current dust up. *See* OFFICE OF THE ATTY GEN., DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996, https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996 (last accessed June 27, 2020) (noting that the Justice Department held a public workshop to discuss the issue of Section 230 reforms on February 19, 2020); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 101, 103 (2008) (finding that "the current regime privileges access providers over both individual speakers and third parties harmed by those speakers' speech. Sometimes that is a mistake, and it is not one that the First Amendment bars us from correcting.").

[238] *See, e.g.*, Limiting Section 230 Immunity to Good Samaritans Act, S.3983, 116th Cong. (2020); Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act of 2019, S.2111, 116th Cong. (2019).

Also, the Department of Justice's Office of the Attorney General recently issued a review of Section 230 identifying "areas ripe for reform."[239] Among the Department's recommendations is "exempting from immunity specific categories of claims that address particularly egregious content, including . . . terrorism."[240] Of course, recommendations from the Office of the Attorney General have no legal—and possibly no persuasive—effect. But the Department's attention to the possible political or legal desirability of a terrorism carve-out shows that government leaders continue to grapple with the appropriate balance of legal rights and protections for terror victims and valuable, powerful internet companies.

But even if the statutory hurdle is lowered or removed, material support claims based on social media algorithms will remain challenging. Assuming Facebook's algorithm is speech, it's unlikely the Supreme Court, applying strict scrutiny, would find the material support statute's civil liability provision constitutional as applied to claims based on independent speech like this. And the proximate causation hurdle presented by the ATA will remain.[241]

Notwithstanding these obstacles, understanding the hurdles such claimants face is valuable, especially given the current attention focused on § 230(c). Understanding exposure under this theory will help social media companies assess risk and voluntarily structure their activities—algorithmic or otherwise—to minimize liability. Understanding the hurdles such claims face can help victims of terrorist attacks make informed decisions about which claims to pursue and which to forgo. Understanding the complexities of terrorism claims against social media companies can inform Congress as it considers amending Section 230. And finally, understanding this analytical process can help courts considering the tragic claims of terror victim plaintiffs navigate the complicated intersecting statutory and constitutional legal issues they present.

---

[239] OFFICE OF THE ATTY GEN., DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996, https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996 (last visited June 27, 2020); DEPT. OF JUSTICE, OFFICE OF PUBLIC AFFAIRS, *Justice Department Issues Recommendations for Section 230 Reform*, 20-556 (June 17, 2020).

[240] OFFICE OF THE ATTY GEN., DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996, https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996 (last visited June 27, 2020).

[241] *See* Retana v. Twitter, Inc., 419 F. Supp. 3d 989, 995 (N.D. Tex. 2019).