Christen, Circuit Judge:

We address three appeals arising from separate acts of terrorism—one in Paris, one in Istanbul, and one in San Bernardino—in which Nohemi Gonzalez, Nawras Alassaf, Sierra Clayborn, Tin Nguyen, and Nicholas Thalasinos lost their lives. The foreign terrorist organization known as ISIS took responsibility for the attacks in Paris and Istanbul and lauded the attack in San Bernardino after the fact. Plaintiffs are members of the victims' families.

Plaintiffs seek damages pursuant to the Anti-Terrorism Act (ATA), 18 U.S.C. § 2333. The ATA allows United States nationals to recover damages for injuries suffered "by reason of an act of international terrorism," *id.* § 2333(a), but the defendant in these cases is not ISIS. Instead, plaintiffs allege that Google, Twitter, and Facebook are directly and secondarily liable for the five murders at issue in these cases. The complaints allege that defendants' social media platforms allowed ISIS to post videos and other content to communicate the terrorist group's message, to radicalize new recruits, and to generally further its mission. Plaintiffs also claim that Google placed paid advertisements in proximity to ISIS-created content and shared the resulting ad revenue with ISIS. In these and other ways, all three complaints allege defendants are directly liable for committing acts of international terrorism pursuant § 2333(a) of the ATA, and secondarily liable for conspiring with, and aiding and abetting, ISIS's acts of international terrorism pursuant to § 2333(d). ...

I

A

Nohemi Gonzalez, a 23-year-old U.S. citizen, studied in Paris, France during the fall of 2015. On November 13, 2015, when Nohemi was enjoying an evening meal with her friends at a café, three ISIS terrorists—Abdelhamid Abaaoud, Brahim Abdeslam, and Chakib Akrouh—fired into the crowd of diners, killing her. This tragic event occurred within a broader series of attacks perpetrated by ISIS in Paris on November 13. ISIS carried out several suicide bombings and mass shootings in Paris that day, including a massacre at the Bataclan theatre. The day after the Paris Attacks, ISIS claimed responsibility by issuing a written statement and releasing a YouTube video. ...

The *Gonzalez* complaint alleges that YouTube "has become an essential and integral part of ISIS's program of terrorism," and that ISIS uses YouTube to recruit members, plan terrorist attacks, issue terrorist threats, instill fear, and intimidate civilian populations. According to the Gonzalez Plaintiffs, YouTube provides "a unique and powerful tool of communication that enables ISIS to achieve [its] goals."

With regard to the Paris Attacks in particular, the Gonzalez Plaintiffs allege that two of the twelve ISIS terrorists who carried out the attacks used online social media platforms to post links to ISIS recruitment YouTube videos and "*jihadi* YouTube videos." Abaaoud, one of the attackers in the café shooting, appeared in an ISIS YouTube video from March 2014, and delivered a monologue aimed at recruiting *jihadi* fighters to join ISIS.

The Gonzalez Plaintiffs' theory of liability generally arises from Google's recommendations of content to users. These recommendations are based upon the content and "what is known about the viewer." Specifically, the complaint alleges Google uses computer algorithms to match and suggest content to users based

upon their viewing history. The Gonzalez Plaintiffs allege that, in this way, Google has "recommended ISIS videos to users" and enabled users to "locate other videos and accounts related to ISIS," and that by doing so, Google assists ISIS in spreading its message. The Gonzalez Plaintiffs' theory is that YouTube is "useful in facilitating social networking among jihadists" because it provides "the ability to exchange comments about videos and to send private messages to other users." ...

According to the Gonzalez Plaintiffs, Google is aware of ISIS's presence on YouTube, has received complaints about ISIS content, has the ability to remove ISIS content from YouTube, and has "suspended or blocked selected ISIS-related accounts at various times." The complaint asserts that in spite of Google's knowledge and control, Google "did not make substantial or sustained efforts to ensure that ISIS would not re-establish the accounts using new identifiers." Instead, the Gonzalez Plaintiffs allege, Google sometimes declined to remove ISIS accounts because the content posted by those accounts did not violate YouTube's policies and, on other occasions, Google removed only a portion of the content posted on ISIS-related accounts but permitted the accounts to remain active. ...

[The district court dismissed most of the claims against Google under Section 230.]

III ...

E ...

The Gonzalez Plaintiffs argue that the immunity afforded by § 230 does not bar their claims because § 230 immunizes only those who publish content created by third parties, and their claims are directed to content created by Google. Google responds that the content the TAC challenges was indeed created by third parties—presumably, ISIS—and that the Gonzalez Plaintiffs' claims impermissibly seek to treat Google as a publisher of that content. We affirm the district court's ruling that § 230 bars all of the TAC's claims except to the extent the TAC presents claims premised on the allegation that Google shared advertising revenue with ISIS. ...

1

As to the first element of § 230, the parties do not dispute that Google is an "interactive computer service" provider as defined in 47 U.S.C. § 230(f)(2). We agree.

2

As to the second element, the Gonzalez Plaintiffs argue their claims do not inherently require a court to treat Google as a publisher or speaker. Google responds that the thrust of the Gonzalez Plaintiffs' claims is that Google did not do enough to block or remove content, and that such claims necessarily require the court to treat Google as a publisher. On this point, we agree with Google. ...

The Gonzalez Plaintiffs argue that their claims do not treat Google as a publisher, but instead assert a simple "duty not to support terrorists." They maintain that just as the ATA prohibits a retailer like Wal-Mart "from supplying fertilizer, knives, or even food to ISIS," the ATA prohibits Google from supplying ISIS with a communication platform. The Gonzalez Plaintiffs' characterization of their claim as asserting a "duty not to support terrorists" overlooks that publication itself is the form of support Google allegedly provided to ISIS. ...

Publishing encompasses "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online ... ." *Fair Housing Council Of San Fernando Valley v. Roommates.Com*, 521 F.3d 1157, 1170-71 (9th Cir. 2008) "Publication involves reviewing, editing, and deciding whether to

publish or to withdraw from publication third-party content." *Barnes*, 570 F.3d 1096, 1102 (9th Cir. 2009); *see also Klayman v. Zuckerberg*, 753 F.3d 1354, 1359, 410 U.S. App. D.C. 187 (D.C. Cir. 2014) ("The very essence of publishing is making the decision whether to print or retract a given piece of content … ."). Here, the Gonzalez Plaintiffs assert that Google failed to prevent ISIS from using its platform, and thereby allowed ISIS to disseminate its message of terror. Because the non-revenue sharing claims seek to impose liability for allowing ISIS to place content on the YouTube platform, they seek to treat Google as a publisher.

3

The Gonzalez Plaintiffs argue that Google does more than merely republish content created by third parties; the TAC alleges that Google "creates" and "develops" the ISIS content that appears on YouTube, at least in part, and therefore receives no protection under § 230. … This argument is precluded by this court's § 230 precedents.

The Gonzalez Plaintiffs are correct that § 230 immunity only applies to the extent interactive computer service providers do not also provide the challenged information content. An "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the *creation or development* of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3) (emphasis added).

We have held that a website that "creat[es] or develop[s]" content "by making a material contribution to [its] creation or development" loses § 230 immunity. *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 (9th Cir. 2016). A "material contribution" does not refer to "merely . . . augmenting the content generally, but to materially contributing *to its alleged unlawfulness*." *Roommates*, 521 F.3d at 1167-68 (emphasis added). This test "draw[s] the line at the 'crucial distinction between, on the one hand, taking actions" to display "actionable content and, on the other hand, responsibility for what makes the displayed content [itself] illegal or actionable." *Kimzey*, 836 F.3d at 1269 n.4 (internal quotation marks omitted) (quoting *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398, 413-14 (6th Cir. 2014)). Other circuits have adopted this "material contribution" test, acknowledging that making a material contribution does not mean "merely taking action that is necessary to the display of the allegedly illegal content," but rather, "being responsible for what makes the displayed content allegedly unlawful." *Dirty World Ent.*, 755 F.3d at 410. Absent this sort of "material contribution," Google does not qualify as an "information content provider," and may be eligible for § 230 immunity.

Plainly, an interactive computer service does not create or develop content by merely providing the public with access to its platform. A "website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online." *Kimzey*, 836 F.3d at 1270. Thus, in *Kimzey*, we concluded that a provider does not create or develop content when its website "does absolutely nothing to enhance the defamatory sting of the message beyond the words offered by the third-party user." *Id.*

The Gonzalez Plaintiffs concede that Google did not initially create any ISIS videos, but allege that Google creates the "mosaics" by which that content is delivered. According to the *Gonzalez* TAC, Google makes a material contribution to the unlawfulness of ISIS content by pairing it with selected advertising and other videos because "pairing" enhances user engagement with the underlying content.

Our case law forecloses the argument that this type of pairing vitiates § 230 immunity.

In *Roommates*, we recognized that a website is not transformed into a content creator or developer by virtue of supplying "neutral tools" that deliver content in response to user inputs. *Roommates* relied on our earlier decision in *Carafano v. Metrosplash, Inc.*, 339 F.3d 1119 (9th Cir. 2003), which concerned a prankster's unauthorized creation of a libelous profile impersonating actress Christianne Carafano on an online dating site. *Carafano*, 339 F.3d at 1121-22. Carafano sued the online dating site for invasion of privacy, misappropriation of the right of publicity, defamation, and negligence.

We determined that the dating website in *Carafano* "provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs." *Roommates*, 521 F.3d at 1172. The website was not transformed into the creator or developer of libelous content contained in users' dating profiles, even though its matchmaking functionality allowed that content to be more effectively disseminated. *Carafano* held that the dating website's "decision to structure the information provided by users [in order to] . . . offer additional features, such as 'matching' profiles with similar characteristics" was consistent with § 230 immunity. 339 F.3d at 1124-25. "[S]o long as a third party willingly provides the essential published content, the interactive [computer] service provider receives full immunity regardless of the specific editing or selection process." *Id.* at 1124.

Critically, *Carafano*'s "neutral tools" were neutral because the website did not "encourage the posting of defamatory content" by merely providing a means for users to publish the profiles they created. *Roommates*, 521 F.3d at 1171. "Indeed, the defamatory posting was contrary to the website's express policies." *Id.*

In contrast, the defendant in *Roommates* operated a website for matching renters with prospective tenants that *did* contribute to the alleged illegality. Before users could search listings or post housing opportunities, the website required them to create profiles. *Id.* at 1161. To do so, users were directed through a series of questions to disclose their sex, sexual orientation, and whether they had children. *Id.* They were also required to describe their preferred renter or tenant with respect to these same three criteria, and encouraged to "provide 'Additional Comments' describing themselves and their desired roommate in an open-ended essay." *Id.*

The plaintiffs in *Roommates* alleged that the website operator violated federal and state laws barring discrimination in housing. *Id.* at 1162. The defendant website operator argued that it was entitled to § 230 immunity. *Id.* Our en banc court concluded the website—by requiring users to disclose their sex, sexual orientation, whether they had children, and the traits they preferred in their roommate—was designed to encourage users to post content that violated fair housing laws. *Id.* at 1161, 1164-66. "By requiring subscribers to provide the information as a condition of accessing its service," and requiring subscribers to choose between "a limited set of pre-populated answers" the website became "much more than a passive transmitter," and instead became "the developer, at least in part, of that information." *Id.* at 1166. The *Roommates* website did not employ "neutral tools"; it required users to input discriminatory content as a prerequisite to accessing its tenant-landlord matching service. *See id.* at 1169. The website therefore lost its § 230 immunity with respect to the discriminatory content it prompted, but it retained immunity for generically asking users to provide "Additional Comments" without telling them "what kind of information they should or must include." *Id.* at 1174.

We recently revisited the scope of § 230 immunity in *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093 (9th Cir. 2019). There, an online messaging board called the Experience Project allowed users to share first-person experiences, post and answer questions, and interact with other users about various topics. A user named Wesley Greer posted an inquiry about opportunities to buy heroin, and received a response from another user. A day after meeting up with the responder, Greer died because the heroin he purchased had been laced with fentanyl. Greer's mother filed suit against the website operator, and the website moved to dismiss based on § 230 immunity.

The plaintiff in *Dyroff* argued that the website created and developed online content because the website "used features and functions, including algorithms, to analyze user posts . . . and recommend other user groups." *Id.* at 1098. We concluded "[t]hese functions—recommendations and notifications—[were] tools meant to facilitate the communication and content of others," and "not content in and of themselves." *Id.* The message board in *Dyroff* employed neutral tools similar to the ones challenged by the Gonzalez Plaintiffs. Though we accept as true the TAC's allegation that Google's algorithms recommend ISIS content to users, the algorithms do not treat ISIS-created content differently than any other third-party created content, and thus are entitled to § 230 immunity.

We conclude the TAC does not allege that Google's YouTube service is materially distinguishable from the matchmaking website at issue in *Carafano* or the algorithms employed by the message board in *Dyroff*. It alleges that Google recommends content—including ISIS videos—to users based upon users' viewing history and what is known about the users. The Gonzalez Plaintiffs allege that Google similarly targets users for advertising based on the content they have selected and other information about users. In this way, a user's voluntary actions inform Google about that user's preferences for the types of videos and advertisements the user would like to see. Rather than suggesting matches for dating, Google matches what it knows about users based on their historical actions and sends third-party content to users that Google anticipates they will prefer. This system is certainly more sophisticated than a traditional search engine, which requires users to type in textual queries, but the core principle is the same: Google's algorithms select the particular content provided to a user based on that user's inputs. *See Roommates*, 521 F.3d at 1175 (observing that search engines are immune under § 230 because they provide content in response to a user's queries "with no direct encouragement to perform illegal searches or to publish illegal content").

The *Gonzalez* complaint is devoid of any allegations that Google specifically targeted ISIS content, or designed its website to encourage videos that further the terrorist group's mission. Instead, the Gonzalez Plaintiffs' allegations suggest that Google provided a neutral platform that did not specify or prompt the type of content to be submitted, nor determine particular types of content its algorithms would promote. The Gonzalez Plaintiffs concede Google's policies expressly prohibited the content at issue. Accordingly, the type of algorithm challenged here, without more, is indistinguishable from the one in *Dyroff* and it does not deprive Google of § 230 immunity. …

Our dissenting colleague argues § 230 should not immunize Google from liability for the claims related to its algorithms, which the dissent characterizes as amplifying and contributing to ISIS's originally posted content. …

As we have explained, Google's algorithms function like traditional search engines that select particular content for users based on user inputs. *See Roommates*,

521 F.3d at 1175 (observing search engines are entitled to § 230 immunity because they provide content in response to users' inquires "with no direct encouragement to perform illegal searches or to publish illegal content"). The TAC does not allege that Google's algorithms prompted ISIS to post unlawful content. Nor does the TAC allege that Google's algorithms treated ISIS-created content differently than any other third-party created content. Contrary to the dissent's assertion, we do not hold that "machine-learning algorithms can *never* produce content within the meaning of Section 230." We only reiterate that a website's use of content-neutral algorithms, without more, does not expose it to liability for content posted by a third-party. Under our existing case law, § 230 requires this result.

The dissent concedes algorithms can be neutral, but it argues § 230 immunity should not apply when the published "message itself is the danger." But this is not where Congress drew the line. At the time Congress enacted § 230, many considered it "*impossible* for service providers to screen each of their millions of postings for possible problems." *Carafano*, 339 F.3d at 1124 (emphasis added). Against this backdrop, Congress did not differentiate dangerous, criminal, or obscene content from innocuous content when it drafted § 230(c)(1). Instead, it broadly mandated that "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of *any information* provided by another information content provider." 47 U.S.C. § 230(c)(1) (emphasis added).

We share the dissent's concerns about the breadth of § 230. As the dissent observes, "there is a rising chorus of judicial voices cautioning against an overbroad reading of the scope of Section 230 immunity," and the feasibility of screening for dangerous content is being revisited. For example, websites are leveraging new technologies to detect, flag, and remove large volumes of criminal content such as child pornography. In light of the demonstrated ability to detect and isolate at least some dangerous content, Congress may well decide that more regulation is needed. In the meantime, our decision does not extend what the dissent rightly describes as § 230's sweeping scope. ...

In sum, though we agree the Internet has grown into a sophisticated and powerful global engine the drafters of § 230 could not have foreseen, the decision we reach is dictated by the fact that we are not writing on a blank slate. Congress affirmatively immunized interactive computer service providers that publish the speech or content of others. ...

BERZON, Circuit Judge, concurring:

I concur in the majority opinion in full. I write separately to explain that, although we are bound by Ninth Circuit precedent compelling the outcome in this case, I join the growing chorus of voices calling for a more limited reading of the scope of section 230 immunity. For the reasons compellingly given by Judge Katzmann in his partial dissent in *Force v. Facebook*, 934 F.3d 53 (2d Cir. 2019), if not bound by Circuit precedent I would hold that the term "publisher" under section 230 reaches only traditional activities of publication and distribution—such as deciding whether to publish, withdraw, or alter content—and does not include activities that promote or recommend content or connect content users to each other. I urge this Court to reconsider our precedent *en banc* to the extent that it holds that section 230 extends to the use of machine-learning algorithms to recommend content and connections to users. ...

The key issue as to the non-revenue-sharing claims in *Gonzalez v. Google* is whether Google, through YouTube, is being treated "as a publisher" of videos posted by ISIS for purposes of these claims. We have previously held that "publication

involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Barnes*, 570 F.3d at 1102. A website's decisions to moderate content, restrict users, or allow third parties full freedom to post content and interact with each other all therefore fall squarely within the actions of a publisher shielded from liability under section 230.

But the conduct of the website operators here—like the conduct of most social media website operators today—goes very much further. The platforms' algorithms suggest new connections between people and groups and recommend long lists of content, targeted at specific users. As Judge Gould's dissent cogently explains, the complaint alleges that the algorithms used by YouTube do not merely publish user content. Instead, they amplify and direct such content, including violent ISIS propaganda, to people the algorithm determines to be interested in or susceptible to those messages and thus willing to stay on the platform to watch more. Similarly, "Facebook uses the algorithms to create and communicate its own message: that it thinks you, the reader—you, specifically—will like this content. And . . . Facebook's suggestions contribute to the creation of real-world social networks." *Force*, 934 F.3d at 82 (Katzmann, C.J., concurring in part and dissenting in part).

In my view, these types of targeted recommendations and affirmative promotion of connections and interactions among otherwise independent users are well outside the scope of traditional publication. Some sites use their algorithms to connect users to specific content and highlight it as recommended, rather than simply distributing the content to anyone who chooses to engage with it. Others suggest that users communicate with designated other users previously unknown to the recipient of the suggestion. Traditional publication has never included selecting the news, opinion pieces, or classified ads to send to each individual reader based on guesses as to their preferences and interests, or suggesting that one reader might like to exchange messages with other readers. The actions of the social network algorithms—assessing a user's prior posts, friends, or viewing habits to recommend new content and connections—are more analogous to the actions of a direct marketer, matchmaker, or recruiter than to those of a publisher. Reading the statute without regard to our post-*Barnes* case law, I would hold that a plaintiff asserting a claim based on the way that website algorithms recommend content or connections to users is not seeking to treat the interactive computer service as a "publisher" within any usual meaning of that term. Instead, the website is engaging in its own communications with users, composing and sending messages to users concerning what they might like to view or who they might like to interact with. ...

BUT: As the majority opinion explains, our case law squarely and irrefutably holds otherwise. There is just no getting around that conclusion, as creatively as Judge Gould's dissent tries to do so. ...

The recommendations and notifications in *Dyroff* are not meaningfully different than the recommendations and connections provided by the social media companies in the cases at issue here. Greer's mother alleged that Experience Project "steered users to additional groups dedicated to the sale and use of narcotics" and "sent users alerts to posts within groups that were dedicated to the sale and use of narcotics," both actions that relied on algorithms to amplify and direct users to content. *Id.* at 1095. Like the recommendations provided by YouTube, Experience Project's recommendations communicated to each user that the website thought that user would be interested in certain posts and topics. And, as here, the

recommended connection was to individuals openly engaged in illegal activity, and the consequences were fatal. Just as the terrorist group's deadly activities were, according to the complaints in these cases, facilitated by recommending their gruesome message to potential recruits, so the drug dealers' illegal activities in *Dyroff* were directly facilitated by connecting them with potential customers. And in both instances, the consequences of the service provider's recommendations were deadly. ...

I therefore concur in full in the majority opinion, as we are bound by this Court's precedent in *Dyroff* extending immunity under section 230 to targeted recommendations of content and connections. But I agree with the dissent and Judge Katzmann that recommendation and social connectivity algorithms—as distinct from the neutral search functions discussed in *Roommates*—provide a "message" from the social media platforms to the user about what content they will be interested in and other people with whom they should connect. Transmitting these messages goes beyond the publishers' role insulated from liability by section 230.

I urge the Court to take this case *en banc* to reconsider our case law and hold that websites' use of machine-generated algorithms to recommend content and contacts are not within the publishing role immunized under section 230. These cases demonstrate the dangers posed by extending section 230 immunity to such algorithmic recommendations, an extension, in my view, compelled by neither the text nor history of the statute. ...

I concur—but, for the reasons stated, reluctantly—in the majority opinion.

GOULD, Circuit Judge, concurring in part and dissenting in part:

I ...

I would hold that Section 230 of the Communications Decency Act does not bar the Gonzalez Plaintiffs' claims for direct and secondary liability under the ATA ...

II ...

The majority ultimately concludes that Section 230 shields Google from liability for its content-generating algorithms. I disagree. I would hold that Plaintiffs' claims do not fall within the ambit of Section 230 because Plaintiffs do not seek to treat Google as a publisher or speaker of the ISIS video propaganda, and the same is true as to the content-generating methods and devices of Facebook and Twitter.

Accepting plausible complaint allegations as true, as we must, Google, through YouTube, and Facebook and Twitter through their various platforms and programs, acted affirmatively to amplify and direct ISIS content, repeatedly putting it in the eyes and ears of persons who were susceptible to acting upon it. For example, YouTube's platform did so by serving up an endless stream of violent propaganda content after any user showed an inclination to view such material. At the same time, it permitted its platforms to be used to convey recruiting information for ISIS-seeking potential terrorists.

Consider how the Google/YouTube algorithm appears to operate: To illustrate, let's assume that a person went to YouTube and asked it to play a favorite song of some artist like Elvis Presley or Linda Ronstadt, or a classical symphony by Ludwig van Beethoven or Wolfgang Amadeus Mozart, or a jazz piece by Miles Davis or Charlie Parker. After that requested song played, the viewer or listener would see automatically a queue of similar or related videos showing either other songs of the requested artist or of some other artists within similar genre. Similarly, if one went to YouTube to see a video about the viewer's favorite National Park, the view-

er would soon see a line of videos about other national parks or similar scenery. And here's the difficulty: If a person asked YouTube to play a video showing one bloody ISIS massacre or attack, other such ISIS attacks would be lined up, or even starting to play automatically. Thus, the seemingly neutral algorithm instead operates as a force to intensify and magnify a message. That poses no problem when the video shows Elvis Presley or Linda Ronstadt performing a musical song, or shows a beautiful National Park. But when it shows acts of the most brutal terrorism imaginable, and those types of images are magnified and repeated over and over again, often coupled with incendiary lectures, then the benign aspects of Google/YouTube, Facebook and Twitter have been transformed into a chillingly effective propaganda device, the results of which were effectively realized in this case. ...

Although Section 230 arguably means that Google and YouTube cannot be liable for the mere content of the posts made by ISIS, that provision in no way provides immunity for other conduct of Google or YouTube or Facebook or Twitter that goes beyond merely publishing the post. ... I would affirm in part to the extent the district court applied Section 230 immunity to YouTube or other platforms simply carrying the posts from ISIS on its platform, but not to the extent that it amplified and in part developed the terrorist message by encouraging similar views to be given to those already determined to be most susceptible to the ISIS cause. ...

I would hold that the Gonzalez Plaintiffs' allegations are more akin to those in *Roommates.com* than *Dyroff* because of the unique threat posed by terrorism compounded by social media. ISIS content on YouTube is a pervasive phenomenon. Plaintiffs allege that "the expansion and success of ISIS is in large part due to its use of the internet and social media platforms to promote and carry out its terrorist activities." One study by the Counter Extremism Project found that between March and June 2018, 1,348 ISIS videos were uploaded to YouTube, garnering 163,391 views. Though websites using neutral tools like algorithms are generally immunized by Section 230, I would hold that where the website (1) knowingly amplifies a message designed to recruit individuals for a criminal purpose, and (2) the dissemination of that message materially contributes to a centralized cause giving rise to a probability of grave harm, then the tools can no longer be considered "neutral." Further, a lack of reasonable review of content posted that

can be expected to be harmful to the public, like ISIS's violent propaganda videos, also destroys neutrality.[5]

In the case of terrorist recruiting, the dissemination itself "contributes materially to the alleged illegality of the conduct," *Roommates.com*, 521 F.3d at 1168, in a way that disseminating other violent videos would not. There can be no doubt that ISIS's use of violence and threats of violence is part of its program of terrorism. Contrary to the majority's contention that Google "merely provided the public with access to its platform," Google affirmatively sent a message in substance to users that individuals who enjoy watching ISIS content may also be interested in joining its ranks. Much as allowing a roommate-matching website to screen candidates by discriminatory criteria presents the same harm as doing such screening in person or by telephone (which is clearly prohibited by statute), a search engine that knowingly transmits recruitment messages to prospective terrorists presents the exact danger—material support to the terrorist cause—that Congress intended to combat with the ATA. Though indeed there are some situations where tools like algorithms can be "neutral," where the message itself is the danger, the tool necessarily contributes to the alleged illegality of the conduct. ...

Furthermore, propagating ISIS messages has an amplification effect that is greater than the sum of each individual connection. Plaintiffs allege that Google does so in part by "using YouTube to direct viewers to other online sites, postings, media, and other social network media." When an ISIS recruitment video manages to reach one person via YouTube that it might not otherwise have reached, that person could join the cause by donating their time, money, or even their life. With each person that joins its ranks, ISIS grows in power and resources. It is the fact of recruitment to a centralized organization with the ability to cause disproportionate harm that distinguishes a terrorist venture from a "normal" criminal venture (as in *Dyroff*). In *Dyroff*, though the website connected Greer with a drug dealer that he might not have otherwise met, the singular connection between the two was unlikely to contribute to a centralized effort to commit international atrocities. I contend that the ATA codifies a duty not to provide material support to terrorism *precisely because* Congress recognized the exponential impact of such conduct. ...

---

5 Google suggests in its briefing that it tries to keep ISIS content from YouTube. But the record in this case suggests that if so, the control has been ineffective. The record shows that despite extensive media coverage, legal warnings, and congressional hearings, social media companies continued to provide a platform and communication services to ISIS before the Paris attacks, and these resources and services went heedlessly to ISIS and its affiliates, as the social media companies refused to actively identify ISIS YouTube accounts, and only reviewed accounts reported by other YouTube users. If, for example, a social media company must take down within a reasonable time sites identified as infringing copyrights, it follows with stronger logic that social media companies should take down propaganda sites of ISIS, once identified, within a reasonable time to avoid death and destruction to the public, which may be victimized by ISIS supporters. Moreover, if social media companies can ban certain speakers who flout their rules by conveying lies or inciting violence, as was widely reported in the aftermath of tweets and posts relating to the recent "insurrection" of January 6, 2021, then it is hard to see why such companies could not police and prohibit the transmission of violent ISIS propaganda videos, in the periods preceding a terrorist attack.

TAAMNEH V. TWITTER, INC.

2 F.4th 871 (9th Cir. 2021)

[This case was heard by the same panel as *Gonzalez* and decided in the same opinion. Because of the procedural posture, however, the issue on appeal was different: whether Twitter could be liable on the merits under the ATA, rather than whether the claims were barred by Section 230.]

Christen, Circuit Judge: ...

Nawras Alassaf, a Jordanian citizen, visited Istanbul, Turkey with his wife to celebrate the 2017 New Year. He was killed on January 1, 2017, when Abdulkadir Masharipov—an individual affiliated with and trained by ISIS—carried out a shooting massacre at the Reina nightclub there (the "Reina Attack"). Masharipov arrived at the Reina nightclub shortly after midnight and, during a seven-minute attack, fired more than 120 rounds into the crowd of 700 people, killing 39 and injuring 69 others. Masharipov escaped the nightclub and evaded arrest for over two weeks but was ultimately apprehended. On the day after the attack, ISIS issued a statement claiming responsibility for the Reina Attack. [Alassaf's relatives' brought ATA claims against Twitter, Facebook, and Google. The district court dismissed these claims on the merits, without reaching the Section 230 issue.]

Under § 2333(d)(2) of the ATA, "liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance" to "the person who committed ... an act of international terrorism" as set forth in § 2333(a). 18 U.S.C. § 2333(d)(2). JASTA specifies that the D.C. Circuit's decision in *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983), describes "the proper legal framework" for assessing aiding-and-abetting liability under § 2333(d). Pub. L. No. 144-222, § 2(a)(5), 130 Stat. at 852. ...

In *Halberstam*, the D.C. Circuit identified three elements that a plaintiff must prove in order to establish aiding-and-abetting liability: "(1) the party whom the defendant aids must perform a wrongful act that causes an injury; (2) the defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance; [and] (3) the defendant must knowingly and substantially assist the principal violation." 705 F.2d at 477.

The Taamneh Plaintiffs adequately allege that defendants knowingly assisted ISIS. Specifically, the FAC alleges that ISIS depends on Twitter, Facebook, and YouTube to recruit individuals to join ISIS, to promote its terrorist agenda, to solicit donations, to threaten and intimidate civilian populations, and to inspire violence and other terrorist activities. The Taamneh Plaintiffs' complaint alleges that each defendant has been aware of ISIS's use of their respective social media platforms for many years—through media reports, statements from U.S. government officials, and threatened lawsuits—but have refused to take meaningful steps to prevent that use. The FAC further alleges that Google shared revenue with ISIS by reviewing and approving ISIS's YouTube videos for monetization through the AdSense program. Taken as true, these allegations sufficiently allege that defendants' assistance to ISIS was knowing.

We next consider whether the Taamneh Plaintiffs plausibly allege that defendants' assistance was "substantial," applying the six *Halberstam* factors. First, the act encouraged is ISIS's terrorism campaign, and the FAC alleges that this enterprise was heavily dependent on social media platforms to recruit members, to raise funds, and to disseminate propaganda. The FAC alleges that by providing ISIS with access to robust communications platforms free of charge, defendants facilitated ISIS's ability to reach and engage audiences it could not otherwise reach, and

served as a matchmaker for people around the globe who were sympathetic to ISIS's vision. It also alleges ISIS's terrorist enterprise relies on financial support, as any money provided to the organization may aid its unlawful goals.

The second factor—the amount of assistance given by a defendant—is addressed by the Taamneh Plaintiffs' allegation that the social media platforms were essential to ISIS's growth and expansion. The Taamneh Plaintiffs allege that, without the social media platforms, ISIS would have no means of radicalizing recruits beyond ISIS's territorial borders. Before the era of social media, ISIS's predecessors were limited to releasing short, low-quality videos on websites that could handle only limited traffic. According to the FAC, ISIS recognized the power of defendants' platforms, which were offered free of charge, and exploited them. ISIS formed its own media divisions and production companies aimed at producing highly stylized, professional-quality propaganda. The FAC further alleges that defendants' social media platforms were instrumental in allowing ISIS to instill fear and terror in civilian populations. By using defendants' platforms, the Taamneh Plaintiffs allege that ISIS has expanded its reach and raised its profile beyond that of other terrorist groups. These are plausible allegations that the assistance provided by defendants' social media platforms was integral to ISIS's expansion, and to its success as a terrorist organization.

The third factor considers the defendant's presence or absence at the time of the tort. At oral argument, Taamneh Plaintiffs unambiguously conceded the act of international terrorism they allege is the Reina Attack itself. There is no dispute that defendants were not present during the Reina Attack.

Fourth, we consider the defendant's relation to the principal actor, ISIS. The FAC indicates that defendants made their platforms available to members of the public, and that billions of people around the world use defendants' platforms. By making their platforms generally available to the market, defendants allowed ISIS to exploit their platforms; but like the *Gonzalez* TAC, these allegations indicate that defendants had, at most, an arms-length transactional relationship with ISIS. The alleged relationship may be even further attenuated than the ones defendants have with some of their other users because the FAC alleges defendants regularly removed ISIS content and ISIS-affiliated accounts. The Taamneh Plaintiffs do not dispute that defendants' policies prohibit posting content that promotes terrorist activity or other forms of violence.

The fifth factor concerns the defendant's state of mind. Here, the Taamneh Plaintiffs do not allege that defendants had any intent to further or aid ISIS's terrorist activities, or that defendants shared any of ISIS's objectives. Indeed, the record indicates that defendants took steps to remove ISIS-affiliated accounts and videos. With respect to advertisements on ISIS YouTube videos, the articles incorporated into the complaint suggest that Google took at least some steps to prevent ads from appearing on ISIS videos.

The sixth factor addresses the period of the defendant's assistance. The Taamneh Plaintiffs allege that defendants provided ISIS with an effective online communications platforms for many years. The FAC alleges that ISIS-affiliated accounts first appeared on Twitter in 2010. According to the Taamneh Plaintiffs' FAC, ISIS used Facebook as early as 2012, and used YouTube as early as 2013.

Taking the FAC's allegations as true, we conclude the Taamneh Plaintiffs adequately allege that defendants' assistance to ISIS was substantial. The FAC alleges that defendants provided services that were central to ISIS's growth and expansion, and that this assistance was provided over many years. ...

NOTE ON SUBSEQUENT HISTORY

In *Gonzalez*, the plaintiffs petitioned the Supreme Court for a writ of certiorari on the question:

> Does section 230(c)(1) immunize interactive computer services when they make targeted recommendations of information provided by another information content provider, or only limit the liability of interactive computer services when they engage in traditional editorial functions (such as deciding whether to display or withdraw) with regard to such information?

Meanwhile, in *Taamneh*, Twitter petitioned the Supreme Court for a writ of certiorari, explaining:

> The Court should deny certiorari in *Gonzalez*. If it does, that decision will also resolve this case. Because the two cases are materially indistinguishable, the parties here have stipulated to dismissal of this action if this Court denies the *Gonzalez* certiorari petition. But in the event the Court grants certiorari in *Gonzalez*, it should also grant in this case. To the extent the claim in this case can proceed notwithstanding Section 230, the Ninth Circuit's misguided interpretation and application of the ATA's aiding-and-abetting provision warrants review.

On October 3, 2022, the Supreme Court granted the petitions in both cases.