FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

REYNALDO GONZALEZ; THE ESTATE OF NOHEMI GONZALEZ; BEATRIZ GONZALEZ, Individually and as Administrator of the Estate of Nohemi Gonzalez; JOSE HERNANDEZ; REY GONZALEZ; PAUL GONZALEZ, *Plaintiffs-Appellants*, v. GOOGLE LLC, *Defendant-Appellee.*	No. 18-16700 D.C. No. 4:16-cv-03282-DMR

Appeal from the United States District Court
for the Northern District of California
Donna M. Ryu, Magistrate Judge, Presiding

MEHIER TAAMNEH; LAWRENCE TAAMNEH; SARA TAAMNEH; DIMANA TAAMNEH, *Plaintiffs-Appellants*, v. TWITTER, INC.; GOOGLE LLC; FACEBOOK, INC., *Defendants-Appellees.*	No. 18-17192 D.C. No. 3:17-cv-04107-EMC

Appeal from the United States District Court
for the Northern District of California
Edward M. Chen, District Judge, Presiding

GREGORY CLAYBORN, Individually and as Successor-In-Interest of the Estate of SIERRA CLAYBORN; KIM CLAYBORN; TAMISHIA CLAYBORN; VANESSA NGUYEN, Individually and as Successor-In-Interest of the Estate of TIN NGUYEN; TRUNG DO; JACOB THALASINOS; JAMES THALASINOS,
Plaintiffs-Appellants,

v.

TWITTER, INC.; FACEBOOK, INC.; GOOGLE LLC,
Defendants-Appellees.

No. 19-15043

D.C. Nos.
3:17-cv-06894-LB
3:18-cv-00543-LB

OPINION

Appeal from the United States District Court
for the Northern District of California
Laurel D. Beeler, Magistrate Judge, Presiding

Argued and Submitted March 26, 2020
San Francisco, California

Filed June 22, 2021

Before: Ronald M. Gould, Marsha S. Berzon, and Morgan Christen, Circuit Judges.

Opinion by Judge Christen;
Concurrence by Judge Berzon;
Partial Concurrence and Partial Dissent by Judge Gould

SUMMARY*

Anti-Terrorism Act

The panel addressed appeals from the district court's dismissal of three actions seeking damages under the Anti-Terrorism Act against Google, Twitter, and Facebook on the basis 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. The panel affirmed the judgments in the *Gonzalez* and *Clayborn* appeals and reversed and remanded in *Taamneh*.

Members of the families of victims of terrorism in Paris, Istanbul, and San Bernardino alleged that Google, Twitter, and Facebook were directly and secondarily liable for ISIS's acts of international terrorism. The *Gonzalez* plaintiffs brought claims for both direct and secondary liability against Google. The district court concluded that most of plaintiffs' claims were barred pursuant to 47 U.S.C. § 230 of the Communications Decency Act, and the direct liability claims failed to adequately allege proximate cause. In the *Taamneh* and *Clayborn* cases, the district court concluded that plaintiffs failed to plausibly allege a secondary liability claim against Google, Twitter, and Facebook.

The panel held that the district court in *Gonzalez* properly ruled that § 230 barred most of plaintiffs' claims. The panel further held that the *Gonzalez* plaintiffs failed to state an

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

actionable claim as to their remaining theories of liability. In *Taamneh*, the panel held that the district court erred by ruling that plaintiffs failed to state a claim for aiding-and-abetting liability under the ATA. In *Clayborn*, the panel concluded that the district court correctly held that plaintiffs failed to plausibly plead their claim for aiding-and-abetting liability.

Addressing *Gonzalez*, the panel held that the civil remedies section of the ATA permits United States nationals to recover damages for injuries suffered "by reason of acts of international terrorism." The Justice Against Sponsors of International Terrorism Act of 2016 (JASTA) amended the ATA to include secondary civil liability for aiding and abetting, or conspiring to commit, acts of international terrorism. Section 230 of the Communications Decency Act protects websites from liability for material posted on the website by someone else. The panel held that the presumption against the extraterritorial application of federal statutes did not prevent § 230 from applying to the *Gonzalez* plaintiffs' claims because the relevant conduct took place in the United States. The panel concluded that JASTA did not impliedly repeal § 230. Agreeing with the First and Second Circuits, the panel held that the exception set forth in § 230(e)(1), concerning impairment of the enforcement of federal criminal statutes, does not extend to actions for civil damages. Thus, the *Gonzalez* plaintiffs' claims were not categorically excluded from the reach of § 230 immunity.

The *Gonzalez* plaintiffs argued that the immunity afforded by § 230 did not bar their claims because § 230 immunizes only those who publish content created by third parties, and their claims were directed to content created by Google. Google argued that the plaintiffs impermissibly sought to treat Google as a publisher of content created by third parties,

presumably ISIS, on YouTube. In Part III.E of its opinion, the panel affirmed the district court's ruling that § 230 barred all of plaintiffs' claims except to the extent their complaint presented claims premised on the allegation that Google shared advertising revenue with ISIS. Section 230(c) precludes liability for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat . . . as a publisher or speaker (3) of information provided by another information content provider." The panel concluded that plaintiffs' claims did not inherently require the court to treat Google as the publisher or speaker of content provided by ISIS, and the duty that plaintiffs alleged Google violated did not derive from Google's status or conduct as a publisher or speaker. The panel concluded that Google did not create or develop content by making a material contribution to its alleged unlawfulness when it created the "mosaics" by which ISIS videos were delivered. The panel held that the court's case law foreclosed the argument that Google's pairing of ISIS content with selected advertising and other videos vitiated § 230 immunity. Accepting as true plaintiffs' allegation that Google's algorithms recommended ISIS content to users, and agreeing with the Second Circuit, the panel wrote that the algorithms did not treat ISIS-created content differently than any other third-party created content, and thus were entitled to § 230 immunity.

In Part III.F of its opinion, the panel held that § 230 did not bar the *Gonzalez* plaintiffs' claims premised on the allegation that because it shared advertising revenue with ISIS, Google should be held directly liable for providing material support to ISIS and secondarily liable for providing substantial assistance to ISIS.

In Parts IV and V, the panel held that the *Gonzalez* plaintiffs did not adequately allege claims for direct or secondary liability under the ATA based on a revenue-sharing theory. As to direct liability, plaintiffs failed to plausibly allege that Google directly perpetrated an act of international terrorism because they did not allege that Google's actions were motivated by anything other than economic self-enrichment. As to secondary liability, plaintiffs did not state a claim on either a theory of aiding and abetting or a theory of conspiracy liability.

In Part VI, reversing the district court's dismissal of the *Taamneh* action, the panel held that the *Taamneh* plaintiffs adequately stated a claim for aiding-and-abetting liability.

In Part VII, affirming the dismissal of the *Clayborn* action, the panel held that because the *Clayborn* plaintiffs did not plausibly allege that ISIS committed, planned or authorized the terrorist attack in San Bernardino, they did not adequately state a claim for aiding and abetting an act of international terrorism.

Judge Berzon concurred in the majority opinion in full. She wrote separately to explain that, although the panel was bound by Ninth Circuit precedent compelling the outcome in this case, she joined the growing chorus of voices calling for a more limited reading of the scope of § 230 immunity. Judge Berzon urged the court to reconsider its precedent en banc to the extent that it holds that § 230 immunity extends to the use of machine-learning algorithms to recommend content and connections to users.

Judge Gould concurred in the majority opinion in its Parts I and II, Part III.A through III.D, Part III.F, and Part VI and

dissented in part as to Part III.E and Parts IV, V, and VII. Judge Gould wrote that he concurred insofar as the majority would reverse in part the dismissal of revenue-sharing claims in *Gonzalez*, and insofar as it would reverse the district court's judgment in *Taamneh* that the complaint failed to adequately state a claim under the ATA. Judge Gould wrote that he dissented as to the majority's dismissal of the *Gonzalez* claims on grounds of § 230 immunity, and of failure to state a claim for direct or secondary liability under the ATA, because of the majority's mistaken conclusion that there was no act of international terrorism, and he also would hold that the complaint adequately alleged that there was proximate cause supporting damages on those claims. Judge Gould agreed that claims could proceed in the *Taamneh* case, and accordingly agreed with reversing and remanding in that case. On the *Clayborn* case, Judge Gould dissented because the majority's conception of an attack authorized by ISIS was inconsistent with the allegations of the operative complaint and well-established principles of tort and agency law.

COUNSEL

Keith Altman (argued) and Daniel W. Weininger (argued), Excolo Law, Southfield, Michigan, Plaintiffs-Appellants Reynaldo Gonzalez, Mehier Taamneh, Lawrence Taamneh, Sara Taamneh, Dimana Taamneh, Gregory Clayborn, Kim Clayborn, Tamishia Clayborn, Vanessa Nguyen, Trung Do, Jacob Thalasinos, and James Thalasinos.

Robert J. Tolchin (argued) and Meir Katz, Berkman Law Office LLC, Brooklyn, New York; for Plaintiffs-Appellants Estate of Nohemi Gonzalez; Beatriz Gonzalez, Jose Hernandez, Rey Gonzalez, and Paul Gonzalez.

Brian M. Willen (argued), Wilson Sonsini Goodrich & Rosati, New York, New York; David H. Kramer, Lauren Gallo White, and Kelly M. Knoll, Wilson Sonsini Goodrich & Rosati, Palo Alto, California; for Defendant-Appellee Google LLC.

Kristin A. Linsley (argued) and Jacob T. Spencer, Gibson Dunn & Crutcher LLP, San Francisco, California; for Defendant-Appellee Facebook Inc.

Seth P. Waxman, Patrick J. Carome, and Ari Holtzblatt, Wilmer Cutler Pickering Hale & Dorr LLP, Washington, D.C., for Defendant-Appellee Twitter Inc.

Aaron Mackey and Sophia Cope, Electronic Frontier Foundation, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

OPINION

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 to § 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).[1]

This opinion addresses three separate appeals. The *Gonzalez* appeal concerns claims for both direct and secondary liability against Google. In that case, the district court granted Google's motion to dismiss, concluding that most of the Gonzalez Plaintiffs' claims were barred pursuant to 47 U.S.C. § 230 of the Communications Decency Act (CDA), and that the Gonzalez Plaintiffs' direct liability claims failed to adequately allege proximate cause. The *Taamneh* and *Clayborn* appeals concern claims for secondary liability against Google, Twitter, and Facebook. In both of these cases, the district court granted defendants' motions to dismiss on the grounds that the plaintiffs failed to plausibly allege a secondary liability claim under the ATA.

We have jurisdiction pursuant to 28 U.S.C. § 1291. We conclude the district court in *Gonzalez* properly ruled that § 230 bars most of the Gonzalez Plaintiffs' claims, and that the Gonzalez Plaintiffs failed to state an actionable claim as to their remaining theories of liability asserted pursuant to the ATA. In *Taamneh*, we conclude the district court erred by ruling the Plaintiffs failed to state a claim for aiding-and-abetting liability under the ATA. The district court did not reach § 230 immunity in *Taamneh*. In *Clayborn*, we conclude the district court correctly held that Plaintiffs failed

[1] The acronym "ISIS" refers to "The Islamic State of Iraq and Syria." ISIS is occasionally referred to as "ISIL" or "The Islamic State of Iraq and the Levant." Both names are derived from the Arabic "ad-Dawlah al-Islamiyah fil-'Iraq wash-Sham." The organization later shortened its name to "ad-Dawlah al-Islamiyah" ("The Islamic State" or "IS"). For simplicity, we use the name ISIS.

to plausibly plead their claim for aiding-and-abetting liability. We therefore affirm the judgments in *Gonzalez* and *Clayborn*, and reverse and remand for further proceedings in *Taamneh*.

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 (the "Paris Attacks"). 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 operative *Gonzalez* complaint alleges that at the time of the Paris Attacks, ISIS had become one of the largest and most widely recognized terrorist organizations in the world. The complaint also alleges that ISIS carried out violent terrorist attacks as a means of instilling terror in the public and communicating its broader objectives, and that ISIS's messages—communicated before, during and after its terror attacks—are essential components of generating the physical, emotional, and psychological impact ISIS desires to achieve.

Google owns YouTube, a global online service used to post, share, view, and comment on videos related to a vast range of topics. Users can post content directly on YouTube,

though Google has the ability to remove any content. When Google receives a complaint about a video, it reviews the video and removes it if it violates Google's content policies.

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 "[t]he ability to exchange comments about videos and to send private messages to other users."

The complaint also asserts that Google pairs videos with advertisements and that it targets advertisements based on information about the advertisement, the user, and the posted video. The complaint alleges that by doing so, Google exercises control over which advertisements are matched with videos posted by ISIS on YouTube, creating new unique content for viewers "by choosing which advertisement to combine with the posted video with knowledge about the viewer."

The Gonzalez Plaintiffs' complaint also alleges that Google's practice is to share a percentage of the revenue it generates from these ads with the users who post the videos. Specifically, the complaint alleges that Google "reviewed and approved ISIS videos, including videos posted by ISIS-affiliated users, for monetization through" its placement of ads on those videos, thereby agreeing to share revenue with ISIS and ISIS-affiliated 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.[2]

Reynaldo Gonzalez, Nohemi's father, filed an action against Google, Twitter, and Facebook on June 14, 2016, and a Second Amended Complaint (SAC) on April 21, 2017. The SAC joined additional family members and named only Google as a defendant. According to the SAC, Google aided and abetted international terrorism and provided material support to international terrorism by allowing ISIS to use YouTube. *See* 18 U.S.C. § 2333(a), (d). Claims One and Two alleged that Google is secondarily liable for aiding and abetting acts of international terrorism and for conspiring with ISIS; Claims Three and Four alleged that Google is directly liable for providing material support and resources to ISIS. Google moved to dismiss all of the Gonzalez Plaintiffs' claims on the grounds that they were barred by § 230 of the CDA. *See* 47 U.S.C. § 230(c). The district court granted the motion to dismiss, but gave the Gonzalez Plaintiffs an opportunity to amend.

The Third Amended Complaint (TAC) is the operative complaint. In it, the Gonzalez Plaintiffs added additional claims. The Plaintiffs allege that Google is secondarily liable for Nohemi's death because Google aided and abetted an act of international terrorism and engaged in a conspiracy with a

[2] The Gonzalez Plaintiffs also allege that "Google has tools by which it can identify, flag, review, and remove ISIS YouTube accounts," but improperly focuses primarily "on whether the content posted violates Google's own 'Community Standards,' rather than examin[ing] whether the account is being used by or for the benefit" of terrorists. They further allege that "[e]ven when Google occasionally deletes an account for violating its Community Standards, it allows these accounts to be quickly regenerated."

perpetrator of an act of international terrorism. The *Gonzalez* TAC also alleges that Google is directly liable under § 2333(a) for providing material support and resources to ISIS, and for concealing this support, in violation of 18 U.S.C. §§ 2339A, 2339B(a)(1), and 2339C(c).[3]

Google moved to dismiss the entire TAC based on § 230 immunity, and alternatively moved to dismiss the § 2333(a) direct liability claims (Claims Three through Six) on the ground that they failed to plausibly allege Google proximately caused the Gonzalez Plaintiffs' injury. The district court ruled that all of Plaintiffs' claims were barred by § 230, except to the extent Claims Three and Four were premised on a revenue-sharing theory. The court concluded that Claims Three through Six failed to plausibly allege proximate cause. The revenue-sharing claims were dismissed without prejudice; all the other claims were dismissed with prejudice. The Gonzalez Plaintiffs did not further amend, but they did timely appeal.

B

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

[3] Separately, the Gonzalez Plaintiffs allege that Google provided funds, goods, or services to or for the benefit of global terrorists in violation of Executive Order No. 13224, 31 C.F.R. Part 594, and 50 U.S.C. § 1705.

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.

Twitter is a social networking service that allows users to publicly connect with other users and to distribute content publicly by posting "tweets." The Taamneh Plaintiffs allege that Twitter has the ability to remove tweets and accounts, but does not do so proactively. Instead, Twitter reviews content that is reported by others as violating its rules.

Facebook is also a social networking service that allows users to communicate with other users and to share and distribute content publicly. Facebook has the ability to remove content posted by its users.

The Taamneh Plaintiffs are relatives of Nawras Alassaf. They allege that Google, Twitter, and Facebook were a critical part of ISIS's growth. Much like the *Gonzalez* complaint, the *Taamneh* complaint alleges that ISIS uses defendants' social media platforms to recruit members, issue terrorist threats, spread propaganda, instill fear, and intimidate civilian populations. According to the Taamneh Plaintiffs, ISIS could not have grown into one of the most recognizable and feared terrorist organizations without the effective communications platforms provided by defendants free of charge.

The Taamneh Plaintiffs' complaint alleges that ISIS and its affiliated entities have used YouTube, Twitter, and Facebook for many years with "little or no interference."

"Despite extensive media coverage, complaints, legal warnings, petitions, congressional hearings, and other attention for providing [their] online social media platforms and communications services to ISIS, . . . Defendants continued to provide these resources and services to ISIS and its affiliates." The Taamneh Plaintiffs also allege that defendants knowingly permitted ISIS and its members and affiliates to use their platforms, and reviewed ISIS's use only in response to third-party complaints. The complaint further alleges that even when defendants received complaints about ISIS's use of their platforms, the defendants "have at various times determined that ISIS's use of [their] [s]ervices did not violate Defendants' policies," and therefore "permitted ISIS-affiliated accounts to remain active, or removed only a portion of the content posted on an ISIS-related account . . . ."

The Taamneh Plaintiffs' claims against Google, Twitter, and Facebook allege these defendants aided and abetted an act of international terrorism, conspired with the perpetrator of an act of international terrorism, and provided material support to ISIS, by allowing ISIS to use their social media platforms. Like the Gonzalez Plaintiffs, the Taamneh Plaintiffs allege that defendants' actions violated the ATA. Specifically, the *Taamneh* complaint includes claims for direct and secondary liability under the ATA, 18 U.S.C. § 2333(a), (d), and state-law claims for negligent infliction of emotional distress and wrongful death.

In response to defendants' first motion to dismiss, the Taamneh Plaintiffs amended their complaint once as a matter of right and added additional claims. The First Amended Complaint (FAC) is the operative complaint and it alleges that Google, Twitter, and Facebook are secondarily liable under § 2333(d) for aiding and abetting an act of international

terrorism and for conspiring with a perpetrator of an act of international terrorism. The *Taamneh* complaint also alleges that Google, Twitter, and Facebook are directly liable under § 2333(a) for providing material support and resources to ISIS, and for concealing this support, in violation of 18 U.S.C. §§ 2339A, 2339B(a)(1), and 2339C(c).[4]

Defendants moved to dismiss. The district court ruled the direct liability claims failed to adequately allege proximate cause, and that the secondary liability claims failed to state a claim for conspiracy to commit an act of international terrorism, or for aiding and abetting an act of international terrorism. The court dismissed the complaint with prejudice, and the Taamneh Plaintiffs timely appealed.

C

Sierra Clayborn, Tin Nguyen, and Nicholas Thalasinos attended an office holiday party at the Inland Regional Center in San Bernardino, California on December 2, 2015. Syed Rizwan Farook, a U.S. citizen, and Tashfeen Malik, Farook's wife, entered the building dressed in black and armed with AR-15 semi-automatic rifles, a 9mm handgun, and assembled pipe bombs. Farook and Malik indiscriminately fired more than 100 rounds into the office gathering (the San Bernardino Attack). At some point during the attack, Malik declared on her Facebook page the couples' allegiance and loyalty to former ISIS leader, Abu Bakr al-Baghdadi. Clayborn, Ngyuen, and Thalasinos were among the fourteen people

[4] The Taamneh Plaintiffs' complaint also includes an allegation that Google, Twitter, and Facebook provided funds, goods, or services to or for the benefit of global terrorists in violation of Executive Order No. 13224, 31 C.F.R. Part 594, and 50 U.S.C. § 1705.

murdered in the attack. Twenty-two others were seriously wounded. After the San Bernardino Attack, Farook and Malik fled the scene and were killed in a police shootout. ISIS issued a statement two days later that "[t]wo followers of Islamic State attacked several days ago a center in San Bernardino in California, we pray to God to accept them as Martyrs."

The Clayborn Plaintiffs are relatives of Sierra Clayborn, Tin Nguyen, and Nicholas Thalasinos. Plaintiffs allege that Twitter, Facebook, and Google aided and abetted international terrorism and provided material support to international terrorists in violation of the ATA, by allowing ISIS to use their platforms. The Clayborn Plaintiffs allege Farook and Malik were radicalized by ISIS's use of social media. This complaint includes direct and secondary liability claims against all three defendants pursuant to 18 U.S.C. §§ 2333(a) and (d), 2339A, 2339B, and 2339C, and state-law claims for negligent infliction of emotional distress and wrongful death.

Defendants moved to dismiss. The district court granted the motion and dismissed the Clayborn Plaintiffs' operative complaint on the grounds that the direct liability claims failed to adequately allege proximate cause, and that the secondary liability claims failed to plausibly allege substantial assistance or that ISIS committed, planned, or authorized the San Bernardino Attack. The Clayborn Plaintiffs only appeal the district court's ruling that they failed to adequately plead a secondary liability claim for aiding and abetting international terrorism under 18 U.S.C. § 2333(d).

II

We review de novo a district court's order granting a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), accepting all factual allegations as true and construing them in the light most favorable to the nonmoving party. *Fields v. Twitter, Inc.*, 881 F.3d 739, 743 (9th Cir. 2018).

These appeals concern claims for civil liability under the ATA. The civil remedies section of the ATA permits United States nationals to recover damages for injuries suffered "by reason of an act of international terrorism." 18 U.S.C. § 2333(a). The ATA contains criminal provisions, the violation of which can give rise to a cause of action under § 2333(a) provided other conditions are met. *Fields*, 881 F.3d at 743. Specifically, 18 U.S.C. §§ 2339A, 2339B, and 2339C criminalize providing material support for terrorism, providing material support for foreign terrorist organizations, and financing terrorism, respectively.[5]

[5] Section 2339A(a) prohibits the provision of "material support or resources" by anyone "knowing or intending that they are to be used in preparation for, or in carrying out" any of several enumerated crimes of terrorism. 18 U.S.C. § 2339A(a). Section 2339B(a)(1) prohibits the knowing provision of "material support or resources to a foreign terrorist organization." *Id.* § 2339B(a)(1). Section 2339C(c) prohibits the knowing "conceal[ment] or disguise[] [of] the nature, location, source, ownership, or control" of any support, resources, or funds, knowing that such "support or resources are to be provided, or . . . were provided, in violation of section 2339B." *Id.* § 2339C(c). Executive Order No. 13224, 31 C.F.R. Part 594 and 50 U.S.C. § 1705 generally prohibit providing funds, goods, or services to or for the benefit of designated global terrorists.

"[I]nternational terrorism" is defined in 18 U.S.C. § 2331(1). Acts of international terrorism "involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State." 18 U.S.C. § 2331(1)(A). The acts must "appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping." *Id.* § 2331(1)(B). Finally, the acts must "occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries . . . ." *Id.* § 2331(1)(C).

In 2016, Congress broadened the scope of ATA liability by enacting the Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. No. 144-222, 130 Stat. 852 (2016). JASTA amended the ATA to include secondary civil liability for "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed" an act of international terrorism that was "committed, planned, or authorized" by a foreign terrorist organization. Pub. L. 114-222, § 2(b), 130 Stat. 852, 854 (2016); 18 U.S.C. § 2333(d). Thus, as amended, the ATA allows claims for direct liability for committing acts of international terror pursuant to § 2333(a), or secondary liability pursuant to § 2333(d) for aiding and abetting, or conspiring to commit, acts of international terrorism.

III

These cases share some common issues but took different paths to reach our court. In *Gonzalez*, the district court

primarily relied on § 230 immunity to conclude that all but the Gonzalez Plaintiffs' revenue-sharing claims were barred. The district court separately concluded the revenue-sharing claims failed because the TAC did not plausibly allege that Google proximately caused Nohemi's death. The court allowed the Gonzalez Plaintiffs an opportunity to amend their revenue-sharing claims, but the plaintiffs declined to do so, and final judgment was entered. In *Taamneh* and *Clayborn*, the district courts did not consider § 230 immunity. Instead, the direct liability claims were dismissed for failure to plausibly allege proximate cause, and the secondary liability claims were dismissed for failure to plausibly allege liability for aiding and abetting or conspiracy.

On appeal, the Gonzalez Plaintiffs begin by arguing that § 230 does not apply to their claims at all. They make three arguments in support of this contention: (1) § 230 immunity has no application to extraterritorial claims; (2) Congress impliedly repealed § 230 when it amended the ATA in 2016; and (3) § 230 immunity does not apply to ATA claims based on criminal statutes. Alternatively, the Gonzalez Plaintiffs argue that their claims, both revenue-sharing and those unrelated to revenue-sharing, survive the application of § 230. Finally, the Gonzalez Plaintiffs argue that the TAC adequately states claims for direct and secondary liability under the ATA. The Taamneh Plaintiffs and the Clayborn Plaintiffs argue their complaints adequately allege that defendants violated the ATA by aiding and abetting an act of international terrorism.[6] We begin by considering the

[6] Though the district court did not address the application of § 230 immunity to the Taamneh Plaintiffs' claims, defendants raise § 230 on appeal as an alternative basis for affirmance. We decline to reach this question in the first instance.

application of § 230 immunity to the Gonzalez Plaintiffs' claims.

A

Congress enacted the Communications Decency Act as part of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. Section 230 of the CDA "immunizes providers of interactive computer services against liability arising from content created by third parties." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc) (footnote omitted). Congress designed § 230 "to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1099–1100 (9th Cir. 2009) (quoting *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003)). Congress was concerned with "the ease with which the Internet delivers indecent or offensive material, especially to minors" and sought "to empower interactive computer service providers to self-regulate." *Force v. Facebook, Inc.*, 934 F.3d 53, 78–79 (2d Cir. 2019) (Katzmann, C.J., concurring in part and dissenting in part). To avoid chilling speech, Congress "made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages." *Carafano*, 339 F.3d at 1123 (alteration in original) (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997)).

The operative provision, § 230(c)(1), states "[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." 47 U.S.C. § 230(c)(1). We have said that, "[i]n general, this section protects websites from liability for material posted on the website by someone else." *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016).

Section 230's use of the phrase "publisher or speaker" was prompted by a New York state-court decision that held an internet service provider legally responsible for a defamatory message posted to one of its message boards. *Roommates*, 521 F.3d at 1163 (citing *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished)). *Stratton Oakmont* concluded that the internet service provider "had become a 'publisher' under state law because it voluntarily *deleted* some messages from its message boards 'on the basis of offensiveness and bad taste,' and was therefore legally responsible for the content of defamatory messages that it failed to delete." *Id.* (emphasis added) (internal quotation marks omitted) (quoting *Stratton Oakmont*, 1995 WL 323710, at *4). The original goal of § 230 was modest. By passing § 230, Congress sought to allow interactive computer services "to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete." *Id.*

B

The Gonzalez Plaintiffs first argue that the presumption against the extraterritorial application of federal statutes prevents § 230 from applying to their claims. We disagree.

The presumption against extraterritoriality requires that, "[a]bsent clearly expressed congressional intent to the

contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016). The Supreme Court "has established a two-step framework for deciding questions of extraterritoriality." *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2136 (2018). "The first step asks 'whether the presumption against extraterritoriality has been rebutted.'" *Id.* (quoting *RJR Nabisco*, 136 S. Ct. at 2101). The presumption is rebutted only when "the text [of the statute] provides a 'clear indication of an extraterritorial application.'" *Id.* (quoting *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)). If the presumption is not rebutted by the statute's text, "the second step of [the] framework asks 'whether the case involves a domestic application of the statute.'" *Id.* (quoting *RJR Nabisco*, 136 S. Ct. at 2101). This step requires the court to identify the statute's focus, and ask "whether the conduct relevant to that focus occurred in United States territory." *Id.* "If it did, then the case involves a permissible domestic application of the statute." *Id.*

The Gonzalez Plaintiffs argue that *RJR Nabisco* recognized an exception to this two-step framework where, as here, all relevant conduct takes place outside the United States. To support this proposition, they rely on the Supreme Court's statement in *RJR Nabisco* that "[b]ecause 'all the relevant conduct' regarding those violations 'took place outside the United States,' we did not need to determine . . . the statute's 'focus.'" 136 S. Ct. at 2101 (citation omitted) (quoting *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124 (2013)). The Gonzalez Plaintiffs misread *RJR Nabisco*. The passage they rely upon explained only that, on the facts of *Kiobel*, an inquiry into the focus of the statute was

unnecessary because all the relevant conduct was foreign. *Id.*[7]

The Gonzalez Plaintiffs next argue that even if the *RJR Nabisco* framework is applied, the framework demonstrates that the their claims involve an extraterritorial application of § 230. Again, we are not persuaded.

RJR Nabisco requires that we begin by asking whether the statute "gives a clear, affirmative indication that it applies extraterritorially." 136 S. Ct. at 2101. Neither party identifies any indication that Congress intended § 230 to apply extraterritorially, so we proceed to step two.

At step two, to determine whether claims involve a domestic application of the statute, we must identify "the statute's focus." *Id.* A statute's focus is "the object of its solicitude, which can include the conduct it seeks to regulate, as well as the parties and interests it seeks to protect or vindicate." *WesternGeco*, 138 S. Ct. at 2137 (internal quotations and alterations omitted). "If the conduct relevant to the statute's focus occurred in the United States . . . , then

[7] Google separately argues that because § 230 does not directly regulate conduct, extraterritoriality principles are not implicated at all. The Ninth Circuit addressed a similar situation in a pre-*RJR Nabisco* case. *See Blazevska v. Raytheon Aircraft Co.*, 522 F.3d 948 (9th Cir. 2008). There, our court concluded that the General Aviation Revitalization Act's statute of repose did not "impermissibly regulate conduct that ha[d] occurred abroad." *Id.* at 953. Instead, the statute "merely eliminate[d] the power of any party to bring a suit for damages . . . after the limitation period." *Id.* "Accordingly, the presumption against extraterritoriality simply [was] not implicated . . . ." *Id.* Because we conclude this case does not involve an impermissibly extraterritorial application of law under the *RJR Nabisco* framework, we need not decide the applicability of *Blazevska*. *See also Force*, 934 F.3d at 74.

the case involves a permissible domestic application of the statute." *Id.* at 2136 (internal quotation marks omitted) (quoting *RJR Nabisco*, 136 S. Ct. at 2101).

The object of § 230(c)(1)'s solicitude is to encourage providers of interactive computer services to monitor their websites by limiting liability. *Force*, 934 F.3d at 74 (concluding § 230's "primary purpose is limiting civil liability in American courts"). Section 230 "immunizes providers of interactive computer services against liability arising from content created by third parties." *Roommates*, 521 F.3d at 1162 (footnote omitted); *see also Barnes*, 570 F.3d at 1100 (observing § 230(c)(1) "precludes liability"). This limitation of liability had the dual purposes of "promot[ing] the free exchange of information and ideas over the Internet and . . . encourag[ing] voluntary monitoring for offensive or obscene material." *Carafano*, 339 F.3d 1122. Because the focus of § 230(c)(1) is limiting liability, the conduct relevant to the statute's focus occurs at the location associated with the imposition of liability. *RJR Nabisco*, 136 S. Ct. at 2101.

In other words, because § 230(c)(1) focuses on limiting liability, the relevant conduct occurs where immunity is imposed, which is where Congress intended the limitation of liability to have an effect, rather than the place where the claims principally arose. As such, the conduct relevant to § 230's focus is entirely within the United States—i.e., at the situs of this litigation. *See Force*, 934 F.3d at 74 ("The regulated conduct—the litigation of civil claims in federal courts—occurs entirely domestically in its application here."). We therefore conclude the Gonzalez Plaintiffs' claims involve a domestic application of § 230.

C

The Gonzalez Plaintiffs also argue that § 230 immunity does not shield liability arising from violations of the ATA because § 230 was impliedly repealed. Specifically, they contend that when Congress amended the ATA in 2016 by enacting JASTA, it impliedly repealed § 230. In support of this argument, the Gonzalez Plaintiffs rely on JASTA's statement of purpose, which explains that the aim of the amendment was "to provide civil litigants with the *broadest possible basis*, consistent with the Constitution of the United States, to seek relief" for acts of international terrorism. JASTA § 2(b) (emphasis added). As explained, JASTA altered the ATA by adding, among other things, secondary liability. *See* 18 U.S.C. § 2333(d). Despite its broad purpose, JASTA did not impliedly repeal § 230.

"[A]bsent a clearly expressed congressional intention, repeals by implication are not favored." *Branch v. Smith*, 538 U.S. 254, 273 (2003) (internal quotation marks and citations omitted). "An implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the latter Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'" *Id.* (quoting *Posadas v. Nat'l City Bank*, 296 U.S. 497, 503 (1936)). "Irreconcilable conflict occurs if 'there is a positive repugnancy' between competing provisions or if those provisions cannot 'mutually co-exist.'" *King v. Blue Cross & Blue Shield of Ill.*, 871 F.3d 730, 740 (9th Cir. 2017) (quoting *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976)). "[W]hen two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective." *Id.* (alterations in original) (quoting *Radzanower*, 426 U.S. at 155).

To determine whether JASTA had any effect on the application of § 230, we start by examining the statutory language, and not—as the Gonzalez Plaintiffs urge—JASTA's statement of purpose. Preambles and prefatory language are insufficient to alter the substance of the phrases they precede, even when codified. *See, e.g.*, *Kingdomware Techs., Inc. v. United States*, 136 S. Ct. 1969, 1978 (2016) (observing that the "clause announc[ing] an objective . . . [did] not change the plain meaning of the operative clause"). The Gonzalez Plaintiffs do not identify any substantive provision of JASTA that conflicts with § 230. As we have recognized, § 230 protects from liability only a specific class of defendants facing a particular type of claim—i.e., it protects providers and users of interactive computer services from claims seeking to treat them as publishers or speakers of information provided by others. *See Barnes*, 570 F.3d at 1100–01; *see also* § 230(c)(1). Thus, by its own terms, § 230 creates "an affirmative defense to liability under Section 2333 [of the ATA] for only the narrow set of defendants and conduct to which Section 230 applies." *Force*, 934 F.3d at 72. There is no provision of JASTA to the contrary. JASTA expanded the scope of § 2333 liability for acts of international terrorism, *see* 18 U.S.C. § 2333(d), but it did not modify or repeal § 230 immunity, *Force*, 934 F.3d at 72 ("JASTA merely expanded Section 2333's cause of action to secondary liability; it provides no obstacle . . . to applying Section 230.").

Accordingly, JASTA and § 230(c)(1) can both be enforced without contradicting the other, or depriving the other of "any meaning at all." *Radzanower*, 426 U.S. at 153 (quoting T. Sedgwick, *The Interpretation of Statutory and Constitutional Law* 98 (2d ed. 1874)). Courts have "not hesitated to give effect to two statutes that overlap, so long as

each reaches some distinct cases." *J.E.M. Ag Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc.*, 534 U.S. 124, 144 (2001). Under the Gonzalez Plaintiffs' reading of JASTA, any liability-imposing statute enacted after § 230 would have to be construed to limit § 230 immunity. Such a reading runs directly contrary to the presumption against finding implied repeal. For these reasons, we conclude JASTA did not impliedly repeal § 230.

D

Finally, the Gonzalez Plaintiffs argue that § 230 immunity can never apply to ATA claims because the ATA permits private civil enforcement of counter-terrorism provisions that otherwise give rise to criminal liability, and § 230(e)(1) includes an exception providing that "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute." 47 U.S.C. § 230(e)(1). Google responds that the exception in § 230(e)(1) extends only to criminal prosecutions, not to actions for civil damages like this one. On this point, Google has the better argument.

Courts have consistently held that § 230(e)(1)'s limitation on § 230 immunity extends only to criminal prosecutions, and not to civil actions based on criminal statutes. For example, the First Circuit concluded that a civil remedy provision in the Trafficking Victims Protection Reauthorization Act, which allowed victims to bring suit against perpetrators of sex trafficking, did not fall within the § 230(e)(1) exception. *Doe v. Backpage.com, LLC*, 817 F.3d 12, 23 (1st Cir. 2016). The court principally relied on the meaning of the statutory phrase "enforcement of . . . any . . . Federal criminal statute," which excludes civil statutes, but also reasoned that any ambiguity in the subsection's text was resolved by its title,

"[n]o effect on criminal law," *id.* (alteration in original), because this language "indicate[d] that the provision [was] limited to criminal prosecutions," *id.* The Second Circuit recently agreed with this analysis when it considered the application of § 230 to ATA claims. *See Force*, 934 F.3d at 72 ("We . . . join the First Circuit in concluding that Section 230(e)(1) is 'quite clearly . . . limited to criminal prosecutions.'" (second alteration in original) (quoting *Backpage.com*, 817 F.3d at 23)). We agree with the First and Second Circuits, and hold that § 230(e)(1) is limited to criminal prosecutions. Accordingly, § 230(e)(1) does not preclude the application of § 230(c)(1) immunity.

E

Having concluded that the Gonzalez Plaintiffs' claims are not categorically excluded from the reach of § 230 immunity, we next consider the application of § 230 to the *Gonzalez* TAC. 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.[8]

[8] The Gonzalez Plaintiffs also argue that it was improper for the district court to consider the application of § 230 on a motion to dismiss. We disagree. "Whether a particular ground for opposing a claim may be

Section 230(c)(1) precludes liability for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat . . . as a publisher or speaker (3) of information provided by another information content provider."[9] *Barnes*, 570 F.3d at 1100–01 (footnote omitted). We first address the Gonzalez Plaintiffs' theories of liability that are not directed to revenue-sharing, considering each element of § 230 separately.

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. *Roommates*, 521 F.3d at 1162 n.6 ("[T]he most common interactive computer services are websites."); *see also Kimzey v. Yelp!, Inc.*, 836 F.3d 1263, 1268 (9th Cir. 2016) ("Yelp is plainly a provider of an 'interactive computer service' . . . , a term that

---

the basis for dismissal for failure to state a claim depends on whether the allegations in the complaint suffice to establish that ground." *Jones v. Bock*, 549 U.S. 199, 215 (2007). Here, "the 'allegations in the complaint suffice to establish' the defense," and thus the "affirmative defense may be considered properly." *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013) (quoting *Jones*, 549 U.S. at 215); *see also Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 27 (2d Cir. 2015) (per curiam) (considering whether § 230 immunity barred plaintiffs' claims on a 12(b)(6) motion to dismiss).

[9] *Barnes* limited its summary of § 230(c)(1) eligibility requirements to instances where "plaintiff[s] seeks to treat [the defendant], *under a state law cause of action*, as a publisher or speaker" because that case only concerned state law claims. 570 F.3d at 1100 (emphasis added). In *Roommates*, we acknowledged that § 230 immunity is not limited to cases in which plaintiffs assert state law claims. 521 F.3d at 1164; *see also Barnes*, 570 F.3d at 1100 n.4.

we interpret expansively under the CDA." (quotations and alterations omitted)).

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.

What matters when we assess this element is "whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content provided by another." *Barnes*, 570 F.3d at 1102. This element is satisfied when "the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.'" *Id.*

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. *See Force*, 934 F.3d at 65 (recognizing that supplying a platform and communication services "falls within the heartland of what it means to be the 'publisher' of information under Section 230(c)(1)"). The Plaintiffs' non-

revenue sharing claims seek to impose liability for the content Google allowed to be posted on its platform.

Publishing encompasses "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online . . . ." *Roommates*, 521 F.3d at 1170–71. "[P]ublication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Barnes*, 570 F.3d at 1102; *see also Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014) ("[T]he 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 "creat[es]" and "develop[s]" the ISIS content that appears on YouTube, at least in part, and therefore receives no protection under § 230. Again, we disagree. 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. *Roommates*, 521 F.3d at 1162–63; *see also Carafano*, 339 F.3d at 1123. 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*, 836 F.3d at 1269. 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; *see also, e.g.*, *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 176 (2d Cir. 2016); *Klayman*, 753 F.3d at 1358; *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 257–58 (4th Cir. 2009); *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1197–1201 (10th Cir. 2009). Absent this sort of "material contribution," Google does not qualify as an

"information content provider," and may be eligible for § 230 immunity. *See Kimzey*, 836 F.3d at 1269–70.[10]

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 (quoting *Klayman*, 753 F.3d at 1358). 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.* (quoting *Roommates*, 521 F.3d at 1172).

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.

---

[10] The Gonzalez Plaintiffs argue in passing that the district court erred by "conflat[ing]" the definitions of "creation" and "development" in § 230(f)(3). According to the Gonzalez Plaintiffs, because *Roommates* described its "material contribution" test in the context of construing "development," it "has *nothing* to do with the definition of 'creation.'" Whatever the distinction between creation and development, our case law makes clear that an entity that does not materially contribute to the alleged unlawfulness of the content is neither a creator nor a developer for purposes of § 230(f)(3). *See Kimzey*, 836 F.3d at 1269–70.

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. *See* 521 F.3d at 1171; *see also id.* at 1169; *Kimzey*, 836 F.3d at 1270. *Roommates* relied on our earlier decision in *Carafano*, which concerned a prankster's unauthorized creation of a libelous profile impersonating actress Christianne Carafano on an online dating site. *Roommates*, 521 F.3d at 1171; *see also 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. *Carafano*, 339 F.3d at 1121–22.

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. *See id*. *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. "[I]ndeed, 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. *Id.* at 1094. A user named Wesley Greer posted an inquiry about opportunities to buy heroin, and received a response from another user. *Id.* at 1095. A day after meeting up with the responder, Greer died because the heroin he purchased had been laced with fentanyl. *Id.* Greer's mother filed suit against the website operator, and the website moved to dismiss based on § 230 immunity. *Id.* at 1095–96.

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. *Id.*; *see also Roommates*, 521 F.3d at 1171–72; *Carafano*, 339 F.3d at 1124.

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. *See id.* at 1171. 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.

We are not alone in reaching this conclusion. In a case involving allegations that Facebook unlawfully provided a communications platform to Hamas in violation of the ATA, the Second Circuit concluded that Facebook was entitled to § 230 immunity. *Force*, 934 F.3d at 64–72. The plaintiffs in *Force*, surviving family members of victims allegedly murdered by Hamas, sought to treat Facebook as a publisher of third-party information, even where "it use[d] tools such as algorithms that [were] designed to match that [third-party] information with a consumer's interests." *Id.* at 66. The Second Circuit recognized that Facebook's algorithms may have made content more visible or available, but held this did not amount to *developing* the underlying information. *Id.* at 70. *Force* further observed that since the early days of the Internet, websites "have always decided . . . where on their sites . . . particular third-party content should reside and to whom it should be shown" but no case law denies § 230 immunity "because of the 'matchmaking' results of such editorial decisions." *Id.* at 66–67. Our precedent requires that we reach the same outcome and we hold, consistent with our case law, that Google is entitled to § 230 immunity with respect to the Gonzalez Plaintiffs' theories of liability that are not directed to revenue-sharing.

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. The dissent shares the views expressed by the partial concurrence and

dissent in *Force.* 934 F.3d at 76–89 (Katzmann, C.J., concurring in part, dissenting in part).

As explained, *Force* also arose from terrorist attacks. The *Force* plaintiffs alleged that "Facebook collect[ed] detailed information about its users" and Facebook's algorithms "utilize[d] the collected data to suggest friends, groups, products, services and local events, and [to] target ads based on each user's input." *Id.* at 82 (internal quotation marks omitted).

For two reasons, the partial dissent in *Force* argued that Facebook's friend- and content-suggestion algorithms created new content, and thus Facebook was not entitled to § 230 immunity. *Id.* First, the partial dissent reasoned that Facebook's algorithms communicated their own message—i.e., the algorithms suggested the user would likely be interested in certain additional content. *Id.* Second, Facebook's friend- and content-suggestion algorithms created and maintained "real-world social networks." *Id.*

Citing our circuit's decision in *Roommates*, the partial dissent in *Force* reasoned that suggestions generated by Facebook's algorithms based on users' shared interest in terrorism "directly related to the alleged illegality of the site," and therefore Facebook went beyond the role of a mere publisher. *Id.* at 82–83. Respectfully, this is not a correct reading of *Roommates*. The *Roommates* website required users to identify themselves by sex, sexual orientation, and whether they had children, then directed users to describe their preferred tenant or landlord using pre-populated answers concerning the same criteria. 521 F.3d at 1161, 1169–70. In this way, the website prompted discriminatory responses that violated fair housing laws. *Id.* at 1169–70. Because the

website itself generated the options for selecting a tenant or landlord based on discriminatory criteria, our en banc court concluded the website materially contributed to the unlawfulness of the posted content. *Id.*

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. *See id.* at 1171–72. 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) (quoting *Zeran*, 129 F.3d at 330–31). 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.[11] 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.

[11] According to the Department of Justice, "the vast majority of [National Center for Missing & Exploited Children (NCMEC)] reports come from direct messaging services and are usually generated as a result of platforms' use of automated hashing measures (such as PhotoDNA), grooming indicators, artificial intelligence and other technologies to identify and report child sexual abuse material." DOJ Office of Public Affairs, *Acting AG and Five Country Statement on the Temporary Derogation to the ePrivacy Directive to Combat Child Sexual Exploitation and Abuse*, United States Department of Justice (Jan. 12, 2021), https://www.justice.gov/opa/pr/acting-ag-and-five-country-statement-temporary-derogation-eprivacy-directive-combat-child. Facebook reports that "[i]n addition to photo-matching technology, [Facebook is] using artificial intelligence and machine learning to proactively detect child nudity and previously unknown child exploitative content when it's uploaded" and to report it to NCMEC. *See* Antigone Davis, *New Technology to Fight Child Exploitation*, Facebook (Oct. 24, 2018), https://about.fb.com/news/2018/10/fighting-child-exploitation.

In his partial concurrence and partial dissent in *Force*, Chief Judge Katzmann provided a thorough analysis of § 230's legislative history. *Force*, 934 F.3d at 77–80 (Katzmann, C.J., concurring in part and dissenting in part). The *Force* partial dissent persuasively explains that when it enacted § 230, "Congress was focused squarely on protecting minors from offensive online material" and sought to "provide[] 'Good Samaritan' protections from civil liability for providers or users of an interactive computer service." *Id.* at 79–80 (quoting S. Rep. No. 104-230, at 194 (1996) (Conf. Rep.)). Despite this clear goal, the language Congress adopted in § 230(c)(1) cuts a much wider swath. *Id.* ("Whatever prototypical situation its drafters may have had in mind, § 230(c)(1) does not limit its protection to situations involving 'obscene material' provided by others, instead using the expansive word 'information.'"). Chief Judge Katzmann urged his colleagues to conclude § 230(c)(1) need not be interpreted to immunize websites' friend- and content-suggestion algorithms, but as we explain, Ninth Circuit case law forecloses his argument.

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.[12]

[12] The dissent would create a new federal common law cause of action treating social media companies as makers and sellers of products through forced advertising, thereby circumventing § 230's expansive immunity. Even if we agree Congress should act to narrow the scope of § 230 immunity or regulate the use of neutral algorithms, we are not free to manufacture entirely new causes of action merely because the political branches have not acted. The Supreme Court has explained "[t]he vesting

F

The Gonzalez Plaintiffs' revenue-sharing theory is distinct from the other theories of liability raised in the TAC. This theory is premised on the allegation that because it shared advertising revenue with ISIS, Google should be held directly liable for providing material support to ISIS pursuant to § 2333(a) and secondarily liable for providing substantial assistance to ISIS pursuant to § 2333(d). The district court's order excluded the Gonzalez Plaintiffs' revenue-sharing claims from its application of § 230. On appeal, Google does not separately respond to the Gonzalez Plaintiffs' revenue-sharing claims. Instead, Google lumps all of the TAC's theories together for purposes of its § 230 argument. Based on our review of case law, the question whether § 230 immunizes an interactive computer service provider's revenue-sharing payments appears to be one of first impression for the courts of appeals. We conclude that § 230 does not immunize Google from the claims premised on revenue-sharing.

Plaintiffs allege that Google generates revenue by selling advertising space through its AdSense program, including advertising space that appears on YouTube. Through AdSense, Google sells advertising opportunities and displays advertisements to YouTube viewers accessing other content. Google targets advertisements based on the content of the

---

of jurisdiction in the federal courts does not in and of itself give rise to authority to formulate federal common law . . . nor does the existence of congressional authority under Art. I mean that federal courts are free to develop a common law to govern those areas until Congress acts." *Texas Indus., Inc. v. Radcliff Materials, Inc.*, 451 U.S. 630, 640–41 (1981) (internal citation omitted).

advertisements, what is known about the viewer, and the content of the posted video. If a YouTube user elects to participate in the AdSense program, Google shares with the user a portion of the revenue generated by the advertisements on the user's videos. For example, suppose a user participating in the AdSense program posts a video tutorial about proper house-painting techniques. In this scenario, viewers of the video tutorial might see advertisements for paint or paintbrushes, and Google would share a portion of the resulting ad revenue with the user that posted the video tutorial.

The Gonzalez Plaintiffs allege that "each YouTube video must be reviewed and approved by Google before Google will permit advertisements to be placed with that video," and that "Google has reviewed and approved ISIS videos" for advertising. The Gonzalez Plaintiffs also allege that, because it approved ISIS videos for the AdSense program, Google shared a percentage of revenues generated from those advertisements with ISIS.

We have explained that § 230 grants immunity from claims seeking to hold providers of interactive computer services liable as *publishers or speakers of third-party content*. The Gonzalez Plaintiffs' revenue-sharing allegations are not directed to the publication of third-party information. These allegations are premised on Google providing ISIS with material support by *giving ISIS money*. Thus, unlike the Gonzalez Plaintiffs' other allegations, the revenue-sharing theory does not depend on the particular content ISIS places on YouTube; this theory is solely directed to Google's unlawful payments of money to ISIS.

It is well settled that § 230 "bars only liability that treats a website as a publisher or speaker of content provided by somebody else." *Internet Brands*, 824 F.3d at 851. Perhaps the best indication that the Gonzalez Plaintiffs' revenue-sharing allegations are not directed to any third-party content is that Google's alleged violation of the ATA could be remedied without changing any of the content posted by YouTube's users. *See id.*; *see also HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 683 (9th Cir. 2019) (concluding that a city ordinance that did "not proscribe, mandate, or even discuss the content of the listings that the [plaintiffs] display[ed] on their websites" fell outside the scope of immunity provided by § 230). The Gonzalez Plaintiffs' allegations of revenue-sharing do not seek to hold Google liable for any content provided by a third-party. Accordingly, we conclude that § 230 does not bar the Gonzalez Plaintiffs' claims premised on sharing revenue with ISIS.[13]

IV

Having concluded that § 230 only immunizes Google from liability for all of the Gonzalez Plaintiffs' non-revenue sharing claims, we next address whether, based on the TAC's revenue-sharing theory, the Gonzalez Plaintiffs' adequately allege claims for direct liability and secondary liability under the ATA. We address the direct liability claims first.

[13] The district court dismissed the revenue-sharing claims without prejudice for failure to adequately allege proximate cause. The Gonzalez Plaintiffs chose not to amend, and a final judgment was subsequently entered on that basis.

The civil remedies provision of the ATA, 18 U.S.C. § 2333(a), "allows any United States national 'injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors or heirs,' to sue in federal court and recover treble damages and attorney's fees." *Fields*, 881 F.3d at 743 (quoting § 2333(a)). It is undisputed that the Gonzalez Plaintiffs, Taamneh Plaintiffs, and Clayborn Plaintiffs are United States nationals.

The ATA includes several criminal provisions, "the violation of which can provide the basis for a cause of action under § 2333(a)." *Id.* The Gonzalez Plaintiffs argue that Google directly committed acts of international terrorism by providing material support for terrorism, providing material support for foreign terrorist organizations, and financing terrorism in violation of sections 2339A(a), 2339B(a)(1), and 2339C(c), respectively. They also allege that Google violated Executive Order No. 13224, 31 C.F.R. Part 594, and 50 U.S.C. § 1705.

Section 2333(a) is directed to "act[s] of international terrorism." "[I]nternational terrorism" is statutorily defined in 18 U.S.C. § 2331(1). *See generally Fields*, 881 F.3d at 743 n.3; *Linde v. Arab Bank, PLC*, 882 F.3d 314, 326–27 (2d Cir. 2018). Acts constituting international terrorism must "appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping." *Id.* § 2331(1)(B).

The operative *Gonzalez* complaint contends that Google's conduct qualified as an act of "international terrorism," citing § 2331(1). We conclude their complaint fails to plausibly

allege that Google directly perpetrated an act of international terrorism as required by § 2331(1)(B).

Whether an act appears to be intended to intimidate or coerce a civilian population or to influence or affect a government, "does not depend on the actor's beliefs, but imposes on the actor an objective standard to recognize the apparent intentions of actions." *Weiss v. Nat'l Westminster Bank PLC*, 768 F.3d 202, 207 n.6 (2d Cir. 2014); *see also Boim v. Holy Land Found. for Relief & Dev.*, 549 F.3d 685, 694 (7th Cir. 2008) (en banc) ("[I]t is a matter of external appearance rather than subjective intent, which is internal to the intender.").

The Gonzalez Plaintiffs argue that the knowing provision of resources to a terrorist organization *necessarily* constitutes "international terrorism," and satisfies the requirements identified in § 2331(1)(B). We disagree. Nothing in the statutory scheme suggests that material support always qualifies as international terrorism because such conduct may or may not objectively appear to be intended to intimidate or coerce. Medical assistance rendered to known terrorists by Doctors Without Borders illustrates this point. *See Boim*, 549 F.3d at 699. Such assistance might arguably provide material support to terrorists in violation of § 2339B, but it would not appear to be intended to intimidate or coerce a civilian population, or to affect the conduct of a government. *See id*. To qualify as international terrorism, the defendant's acts must satisfy each of the criteria contained in § 2331(1), *Linde*, 882 F.3d at 325–26; *see also Fields*, 881 F.3d at 743 n.3, and "the provision of material support to a terrorist organization does not invariably equate to an act of international terrorism," *Linde*, 882 F.3d at 326.

The Gonzalez Plaintiffs rely heavily on the Seventh Circuit's en banc decision in *Boim*, but that reliance is misplaced. The issue in *Boim* was whether defendants who had donated money to Hamas and Hamas-affiliated charities—knowing that Hamas used its resources to finance the killing of Israeli Jews—could be held liable under the ATA for Hamas's 1994 murder of an American teenager in Israel. *Boim*, 549 F.3d at 688–690. The en banc court stated that a knowing donor's contributions to Hamas would satisfy the definitional requirements of "international terrorism" set forth in § 2331(1). *Id.* at 690, 694. *Boim* reasoned that "donations to Hamas . . . would enable Hamas to kill or wound, or try to kill" more people in Israel. *Id.* at 694. The Seventh Circuit concluded that such donations would appear to be intended to intimidate or coerce a civilian population because of the foreseeability of these consequences.[14] *Id*. The Gonzalez Plaintiffs' reliance on *Boim* is misplaced because the allegations here are not at all similar to those in *Boim*, which involved voluntary donations specifically and purposefully directed to a foreign terrorist organization.

Taking as true the allegation that Google shared advertising revenue with ISIS as part of its AdSense program, that action does not permit the inference that Google's actions objectively appear to have been intended to intimidate or coerce civilians, or to influence or affect governments. The Seventh Circuit's decision in *Kemper v. Deutsche Bank AG*, 911 F.3d 383 (7th Cir. 2018), illustrates this point. There, the court concluded that the plaintiff failed to plausibly allege

[14] We express no view on whether *Boim* would be decided the same way today. Notably, that decision was issued before Congress enacted JASTA, thereby creating secondary liability for aiding and abetting acts of international terrorism. *See* 18 U.S.C. § 2333(d)(2).

that Deutsche Bank's institution of procedures to evade U.S. sanctions and facilitate Iranian banking transactions qualified as international terrorism. *Id*. at 390. The court reasoned that Deutsche Bank's actions did "not appear intended to intimidate or coerce any civilian population or government" because, "[t]o the objective observer, its interactions with Iranian entities were motivated by economics." *Id.*

Similarly here, the Gonzalez Plaintiffs did not allege that Google's actions were motivated by anything other than economic self-enrichment. The TAC alleges that Google is a commercial service in the business of selling advertising, and that "Google uses the AdSense monetization program to earn revenue, and as an incentive to encourage users to post videos on YouTube." These allegations are easily distinguished from those involving donations to a known terrorist organization. *See Boim*, 549 F.3d at 690, 694. The Gonzalez Plaintiffs did not allege that Google shared ISIS's vision and objectives, nor that Google intended ISIS to succeed in any future acts of terrorism. Rather, the complaint's allegations suggest that Google split ad revenue with ISIS in furtherance of its own financial best interest.

The TAC fails to allege that Google's provision of material support appeared to be intended to intimidate or coerce a civilian population, or to influence or affect a government as required by the ATA. *See* 18 U.S.C. § 2331(1)(B). For this reason, the *Gonzalez* complaint does not adequately allege the requirements necessary to establish direct liability for an act of international terrorism pursuant to § 2333(a), and we need not reach whether the Gonzalez Plaintiffs sufficiently alleged that Google's actions proximately caused Nohemi Gonzalez's death.

V

Turning to the Gonzalez Plaintiffs' secondary liability claims based on revenue-sharing, Google argues that the *Gonzalez* complaint fails to state a claim for secondary liability pursuant to 18 U.S.C. § 2333(d)(2). We agree.[15]

As originally enacted, the ATA allowed only claims alleging direct liability against the perpetrators of acts of international terrorism. *Rothstein v. UBS AG*, 708 F.3d 82, 97 (2d Cir. 2013); *see also Linde*, 882 F.3d at 319–20. In 2016, Congress amended the ATA by enacting JASTA, which extends civil liability to persons who aid and abet by providing substantial assistance to persons who commit acts of international terrorism, and to those who conspire to commit such acts. 18 U.S.C. § 2333(d)(2). Secondary liability for aiding or abetting acts of terrorism applies only when the principal act of international terrorism is "committed, planned, or authorized by an organization . . . designated as a foreign terrorist organization." *Id.*

The Gonzalez Plaintiffs raise claims for both aiding-and-abetting and conspiracy liability. We address these theories separately.

[15] The district court concluded that the Gonzalez Plaintiffs advanced a revenue-sharing theory only with respect to their claims for direct liability. We find the TAC somewhat ambiguous on this point, but assume for purposes of deciding this appeal that the Gonzalez Plaintiffs raised a revenue-sharing theory with respect to both their direct liability and secondary liability claims.

A

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; *see also Siegel v. HSBC N. Am. Holdings, Inc.*, 933 F.3d 217, 223 (2d Cir. 2019).

Halberstam addressed the scope of secondary liability for common law causes of action. *See* 705 F.2d at 474. The plaintiff, Elliott Halberstam, was the widow of Michael Halberstam. *Id.* Michael Halberstam was a physician killed by Bernard Welch during the course of a burglary. *Id*. Halberstam's widow brought a wrongful death action against Linda Hamilton, Welch's live-in girlfriend, alleging that Hamilton was civilly liable for Michael Halberstam's death, both as an aider-abettor and a co-conspirator. *Id.* at 474–76. Hamilton provided assistance to Welch during the course of his multi-year campaign of burglaries, including preparing letters of sale for stolen goods, falsifying tax returns to conceal income derived from stolen goods, maintaining accounts on Welch's behalf, and handling financial transactions. *Id.* at 475, 486, 488. The D.C. Circuit ultimately concluded that Hamilton was civilly liable for Halberstam's death, even though Welch killed Halberstam during a robbery and Hamilton was not present. The court concluded that Hamilton was liable under a conspiracy theory and also an aiding-and-abetting theory. *Id.* at 489.

The scenario presented in *Halberstam* is, to put it mildly, dissimilar to the one at issue here. But Congress selected *Halberstam* as the governing standard for secondary liability ATA claims because *Halberstam* "has been widely recognized as the leading case regarding Federal civil aiding and abetting . . . liability." 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.

1

The first element of aiding and abetting liability requires a showing that the party the defendant aided committed an act of international terrorism that injured the plaintiff. 18 U.S.C. § 2333(d)(2); *Halberstam*, 705 F.2d at 477; *see also Siegel*, 933 F.3d at 223.[16] The parties dispute whether the relevant principal actor is the ISIS organization as a whole or the individual terrorists who perpetrated the Paris Attacks. We agree with the Gonzalez Plaintiffs that ISIS is the relevant

[16] As noted, the ATA's secondary liability provision only applies where a designated "foreign terrorist organization" "committed, planned, or authorized" the act of international terrorism. § 2333(d)(2). The parties do not dispute that the Paris Attacks were an act of international terrorism, nor do they dispute that the killing of Nohemi Gonzalez during the Paris Attacks was an injury to the Gonzalez Plaintiffs.

"person who committed . . . an act of international terrorism." 18 U.S.C. § 2333(d)(2).

The TAC alleges that coordinated teams of ISIS terrorists planned and carried out the Paris Attacks. Specifically, it alleges that the café shooters who murdered Nohemi Gonzalez—Abaaoud, Abdeslam, and Akrouh—were members of ISIS. The Gonzalez Plaintiffs further allege that Abaaoud, the operational leader of the Paris Attacks, traveled to Syria to join ISIS in March 2013, joined ISIS while in Syria, and publicly declared his affiliation with ISIS. We accept as true the allegations that, in 2014, Abaaoud posted a link on his Facebook profile to an ISIS recruiting video in which he described his life and role with ISIS, and, that in 2015, ISIS's English-language magazine, *Dabiq*, featured an interview with Abaaoud. These allegations distinguish the TAC from the claims presented in *Crosby v. Twitter, Inc.*, where the Sixth Circuit rejected the plaintiffs' ATA claims because the complaint contained "no allegations that ISIS was involved with the Pulse Night Club shooting" perpetrated by Omar Mateen. 921 F.3d 617, 626 (6th Cir. 2019); *see also* 18 U.S.C. § 2333(d)(2). We conclude the Gonzalez Plaintiffs satisfied the first element of aiding-and-abetting liability because the TAC plausibly alleged that ISIS, a designated terrorist organization, "committed, planned, or authorized" the Paris Attacks.

2

The second element of aiding-and-abetting liability requires a showing that Google was generally aware of its role in ISIS's terrorist activities at the time it provided assistance to ISIS. 18 U.S.C. § 2333(d)(2); *Halberstam*,

705 F.2d at 477; *see also Linde*, 882 F.3d at 329. The Gonzalez Plaintiffs also satisfied this element.

Just as the *Halberstam* court concluded that Linda Hamilton was generally aware of her role in Bernard Welch's ongoing burglary operation because she "knew about and acted to support" it, the Gonzalez Plaintiffs must plausibly allege that, by sharing revenue with ISIS, Google was aware that it was assuming a role in ISIS's terrorist activities. *See Halberstam*, 705 F.2d at 488; *see also Linde*, 882 F.3d at 329 (requiring a showing that "the bank was 'generally aware' that [by providing financial services,] it was thereby playing a 'role' in Hamas's violent or life-endangering activities" (quoting *Halberstam*, 705 F.2d at 477)). Notably, this element does not require a showing of "the specific intent demanded for criminal aiding and abetting culpability," i.e., an "intent to participate in a criminal scheme as 'something that he wishes to bring about and seek by his action to make it succeed.'" *Linde*, 882 F.3d at 329 (quoting *Rosemond v. United States*, 572 U.S. 65, 76 (2014)). Nor does it require that Google "knew of the specific attacks at issue." *Id.*

The TAC adequately alleges that Google was aware of the role it played in ISIS's terrorist activities. Specifically, the Gonzalez Plaintiffs allege that Google knowingly shared advertising revenue with ISIS and that Google did so despite numerous reports from news organizations that Google placed advertisements on ISIS videos. Under these circumstances, the allegation that Google knowingly gave "fungible dollars to a terrorist organization" plausibly alleges that Google was aware of the role it played in activities that "may be 'dangerous to human life.'" *Cf. Kemper*, 911 F.3d at 390; *see also Fields*, 881 F.3d at 748; *Boim*, 549 F.3d at 693.

We are mindful that "aiding and abetting an *act* of international terrorism requires more than the provision of material support to a designated terrorist *organization*." *Linde*, 882 F.3d at 329. Thus, the *mens rea* required for the general awareness element of secondary liability under § 2333(d) may not be coextensive with the showing required for material support under § 2339B. The latter "requires only knowledge of the organization's connection to terrorism, not intent to further its terrorist activities or awareness that one is playing a role in those activities." *See id.* at 330 (citing *Holder v. Humanitarian L. Project*, 561 U.S. 1, 16–17) (2010); *see also, e.g.*, *Siegel*, 933 F.3d at 224 (concluding plaintiffs failed to plead general awareness with allegations "suggest[ing] that in providing banking services to [a Saudi Arabian bank], HSBC had little reason to suspect that it was assuming a role in [al-Qaeda in Iraq's] terrorist activities"). But here, we are satisfied that the allegations indicating Google knowingly contributed money to ISIS suffice to show that Google understood it played a role in the violent and life-endangering activities undertaken by ISIS, and therefore establish the second element of aiding-and-abetting liability for purposes of § 2333(d)(2).

3

The third element of aiding-and-abetting liability requires that the plaintiff show the defendant knowingly and substantially assisted the act of terrorism that injured the plaintiff. 18 U.S.C. § 2333(d)(2); *see also Halberstam*, 705 F.2d at 488 (holding the defendant must have "knowingly and substantially assist[ed] the principal violation"). This element contains two components: (1) "knowing[]" assistance, and (2) "substantial[]" assistance. *See Halberstam*, 705 F.2d at 477; *see also id.* at 488 (evaluating

whether Linda Hamilton assisted Bernard Welch "with knowledge that he had engaged in illegal acquisition of goods" separate from considering whether her "assistance was 'substantial'").

The *Halberstam* court identified six factors relevant to assessing whether the substantial assistance component is satisfied: "(1) the nature of the act encouraged, (2) the amount of assistance given by defendant, (3) defendant's presence or absence at the time of the tort, (4) defendant's relation to the principal, (5) defendant's state of mind, and (6) the period of defendant's assistance." *Linde*, 882 F.3d at 329 (citing *Halberstam*, 705 F.2d at 483–84).[17]

The parties dispute whether the relevant "principal violation" for analyzing the third element is ISIS's broader campaign of terrorism or the Paris Attacks. *See Halberstam*, 705 F.2d at 488. But *Halberstam* explained that the extent of liability under aiding-and-abetting encompasses foreseeability, such that a defendant "who assists a tortious act may be liable for other reasonably foreseeable acts done in connection with it." 705 F.2d at 484. For example, the common law cases *Halberstam* drew upon established that a

[17] In dicta, the Second Circuit suggested that these factors determine "whether the defendant's assistance was *sufficiently knowing and substantial* to qualify as aiding and abetting." *Linde*, 882 F.3d at 329 n.10 (emphasis added). However, *Halberstam* appears to treat "knowing" assistance as an inquiry separate from "substantial" assistance. *See Halberstam*, 705 F.2d at 478 (explaining that the listed factors aid "in making th[e] determination" of "how much encouragement or assistance is *substantial enough*" (emphasis added)). Indeed, the *Halberstam* court explicitly acknowledged that "the scienter requirement in the third element of aiding-abetting" requires that "an aider-abettor must knowingly assist the underlying violation." *See id.* at 485 n.14.

thirteen-year-old boy who broke into a church with some companions could be held liable for damage to the church caused by his companions' failure to extinguish torches they used to light their way in the church attic. *Id.* at 482–83 (citing *Am. Family Mut. Ins. Co. v. Grim*, 440 P.2d 621, 625–26 (Kan. 1968)). Because the need for lighting could have been anticipated, "the boy who had not used a torch, nor even expected one to be lighted, could be liable for the damage caused by the torches." *Id.* at 483. By contrast, the *Halberstam* court cited an example from the Restatement (Second) of Torts where liability was not imposed: if A supplies wire cutters to B to allow B to unlawfully enter the land of C to recapture chattels belonging to B, and B intentionally sets fire to C's house in the course of his trespass, A is not liable for the destroying the house. *Id.* at 483 n.12 (quoting Restatement (Second) of Torts § 876, cmt. d (1976)).

Halberstam concluded that Linda Hamilton was liable for Welch killing Michael Halberstam because of the nature and extent of her assistance to Welch's illegal burglary enterprise. *Id.* at 488. In the court's view, the killing "was a natural and foreseeable consequence of the activity Hamilton helped Welch to undertake." *Id.* "[W]hen she assisted him, it was enough that she knew he was involved in some type of personal property crime at night—whether as a fence, burglar, or armed robber made no difference—because violence and killing is a foreseeable risk in any of these enterprises." *Id.* We have little difficulty concluding that the Paris Attacks were a foreseeable result of ISIS's broader campaign of terrorism. Accordingly, when assessing whether the TAC satisfies the third element of aiding-and-abetting liability, we consider ISIS's broader campaign of terrorism to be the relevant "principal violation."

Pursuant to § 2333(d)(2), liability attaches to an aider-abettor who "*knowingly provid[es]* substantial assistance." 18 U.S.C. § 2333(d)(2) (emphasis added). Thus, a plaintiff must show that the defendant "knowingly gave 'substantial assistance' to someone who performed wrongful conduct." *Halberstam*, 705 F.2d at 478; *see also id.* at 485 n.14 (noting "the scienter requirement in the third element" addresses the issue of "whether an aider-abettor must knowingly assist the underlying violation").

We conclude that the Gonzalez Plaintiffs adequately allege knowing assistance. The TAC alleges "each YouTube video must be reviewed and approved by Google" before advertisements are placed with that video, and "Google has reviewed and approved ISIS videos . . . for 'monetization,'" and Google therefore "shared revenue with ISIS." The TAC alleges that, prior to the Paris Attacks, numerous news organizations reported on Google's placement of advertisements in or alongside ISIS videos, and Google responded to these media reports by stating it worked to prevent ads from appearing on any video once it determined the content was not appropriate for advertising partners.

In *Halberstam*, the knowledge requirement of the third element was satisfied because Linda Hamilton's actions "were performed knowingly to assist Welch in his illicit trade." 705 F.2d at 486; *see also id.* at 488 (noting that Hamilton had "assisted Welch with knowledge that he had engaged in illegal acquisition of goods"). Here, the Gonzalez Plaintiffs allege that Google reviewed and approved ISIS videos for monetization and thereby knowingly provided ISIS with financial assistance for its terrorist operations. According to the TAC, Google did so despite its awareness that these videos were created by ISIS and posted by ISIS

using known ISIS accounts. Taking these allegations as true, they are sufficient to plausibly allege that Google's assistance was knowing as required by § 2333(d)(2).

That leaves the question whether the Gonzalez Plaintiffs sufficiently allege that Google's assistance was "substantial." Based on our review of the six *Halberstam* factors, we conclude the Gonzalez Plaintiffs did not allege that Google's assistance rose to this level. *See Linde*, 882 F.3d at 329; *see also Halberstam*, 705 F.2d at 483–84.

As to the first factor—the nature of the act encouraged—*Halberstam* explained that the nature of the principal's act "dictates what aid might matter, *i.e.*, be substantial." *Halberstam*, 705 F.2d at 484. For example, verbal support might be of great import when a "defendant's war cry for more blood" contributes to an "assaulter's hysteria," but less important in a case involving a defamation. *See id.* Here, the Gonzalez Plaintiffs allege that Google assisted ISIS's long-running terrorist campaign. Financial support is "indisputably important" to the operation of a terrorist organization, *id.* at 488, and any money provided to the organization may aid its unlawful goals. *Fields*, 881 F.3d at 748; *cf. Siegel*, 933 F.3d at 225.

The second factor considers "the amount of assistance given by the defendant." *Halberstam*, 705 F.2d at 478. This factor recognizes that not all assistance is equally important, s*ee id.* at 484, and the TAC contains no information about the amount of assistance provided by Google. It only alleges that Google shared *some* advertising revenue with ISIS.

Third, we consider the defendant's "presence or absence at the time of the tort" to assess whether the defendant's

assistance was "substantial." *Id.* at 478. The Gonzalez Plaintiffs concede that Google was not present at the time of the Paris Attacks. However, if the relevant tort is viewed as ISIS's broader campaign of terrorism, including the dissemination of propaganda on Google's website before and after the Paris Attacks, Google was arguably present for at least some of the terroristic activities that comprise the "principal violation."

The fourth factor considers the defendant's "relation" to the principal, recognizing that some persons—e.g., those in positions of authority, or members of a larger group—may possess greater powers of suggestion. *Id.* at 478, 484. *Halberstam* also cautioned that courts should be "especially vigilant" in evaluating a spouse's assistance, "so as not to infuse the normal activities of a spouse with the aura of a concerted tort." *Id.* at 484. Google allowed members of ISIS who posted videos on YouTube to opt into AdSense, and by approving ISIS videos for monetization, Google agreed to share some percentage of the resulting advertising revenue with those ISIS members. Thus, the allegations in the TAC describe arms-length business transactions between Google and YouTube users who opted into the AdSense program.

The fifth factor is directed to the defendant's "state of mind." *Id.* at 478. Evidence of a defendant's state of mind may show that a defendant was "one in spirit" with the principal actor. *Id.* at 484. The Gonzalez Plaintiffs do not allege that Google had any intent to finance, promote, or carry out ISIS's terrorist acts. *See Siegel*, 933 F.3d at 225. Nor does the TAC suggest that Google shared any of ISIS's objectives. Instead, the allegations show, at most, that Google intended to profit from the AdSense program. The TAC incorporates by reference articles that indicate Google

took some steps to prevent ads from appearing on ISIS videos.[18]

Finally, the sixth factor concerns the "duration of the assistance provided." *Halberstam*, 705 F.2d at 484. *Halberstam* explained that "[t]he length of time an alleged aider-abettor has been involved with a tortfeasor almost certainly affects the quality and extent of their relationship and probably influences the amount of aid provided as well; additionally, it may afford evidence of the defendant's state of mind." *Id.* Here, the TAC lacks specific allegations about the length of time Google provided assistance to ISIS in the form of revenue-sharing, but it cites several news articles from March 2015 and March 2016 describing the placement of advertisements on YouTube videos posted by ISIS. The TAC also provides an example from a video published on May 28, 2015. Thus, at most, the Gonzalez Plaintiffs allege that advertisements were placed on ISIS's YouTube videos during those periods of time.

We conclude that these allegations fall short of establishing that Google's assistance was sufficiently "substantial" for purposes of § 2333(d)(2) liability. When we review an order granting a 12(b)(6) motion to dismiss we are required to assess whether the allegations in the complaint, taken as true, state a claim of substantial assistance. *See Whitaker v. Tesla Motors, Inc.*, 985 F.3d 1173, 1177 (9th Cir. 2021) ("Our case law does not permit plaintiffs to rely on anticipated discovery to satisfy Rules 8 and 12(b)(6); rather,

[18] *See, e.g.*, *Ads Shown Before YouTube ISIS Videos Catch Companies Off-Guard*, NBC News (Mar. 10, 2015), http://www.nbcnews.com/storyline/isis-terror/ads-shown-isis-videos-youtube-catchcompanies-guard-n320946.

pleadings must assert well-pleaded factual allegations to advance to discovery").

Although monetary support is undoubtedly important to ISIS's terrorism campaign, the TAC is devoid of any allegations about how much assistance Google provided. As such, it does not allow the conclusion that Google's assistance was substantial. Nor do the allegations in the TAC suggest that Google intended to assist ISIS. Accordingly, we conclude the Gonzalez Plaintiffs failed to state a claim for aiding-and-abetting liability under the ATA. We do not consider whether the identified defects in the Gonzalez Plaintiffs' revenue-sharing claims—principally, the absence of any allegation regarding the amount of the shared revenue—could be cured by further amendment because the Gonzalez Plaintiffs were given leave to amend those claims and declined to do so. *See WMX Techs., Inc. v. Miller*, 104 F.3d 1133, 1136 (9th Cir. 1997) (en banc).

B

Section 2333(d)(2) also permits claims for secondary liability "as to any person . . . who conspires with the person who committed . . . an act of international terrorism" as set forth in § 2333(a). As with aiding-and-abetting liability, JASTA specifies that the D.C. Circuit's decision in *Halberstam* provides "the proper legal framework" for assessing conspiracy liability under § 2333(d). Pub. L. No. 144-222, § 2(a)(5), 130 Stat. at 852. *Halberstam* concluded that proof of conspiracy requires three elements: (1) "an agreement to do an unlawful act or a lawful act in an unlawful manner," (2) "an overt act in furtherance of the agreement by someone participating in it," and (3) "injury caused by the act." 705 F.2d at 487. We conclude the Gonzalez Plaintiffs'

TAC does not state an actionable claim for conspiracy liability.

The TAC's allegations are insufficient to plausibly suggest that Google reached an agreement with ISIS to carry out the Paris Attacks that caused Nohemi Gonzalez's death. *Halberstam* requires the overt act causing plaintiffs' injury must be "done pursuant to and in furtherance of the common scheme." *Id.* at 477. Google's sharing of revenues with members of ISIS does not, by itself, support the inference that Google tacitly agreed to commit homicidal terrorist acts with ISIS, where Nohemi Gonzalez's murder was an overt act perpetrated pursuant to, and in furtherance of, that common scheme.[19] We therefore conclude that the Gonzalez Plaintiffs fail to state a claim for conspiracy liability under the ATA, and affirm the district court's dismissal with prejudice of the TAC.

VI

We now turn to the *Taamneh* appeal. As we have explained, although the complaints in *Gonzalez* and *Taamneh* are similar, our decision in *Taamneh* is largely dictated by the path *Taamneh* took to reach our court. Because the bulk of the Gonzalez Plaintiffs' claims were properly dismissed on the basis of § 230 immunity, our decision in *Gonzalez* principally focuses on whether the Gonzalez Plaintiffs'

[19] The Gonzalez Plaintiffs seek to enlist the TAC's allegation that "Google . . . conspired with ISIS, its members[,] and affiliates" to promote, plan, and carry out "the acts of international terrorism that injured the plaintiffs." But this conclusory allegation is insufficient to survive a motion to dismiss. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007).

revenue-sharing theory sufficed to state a claim under the ATA. In contrast, the district court in *Taamneh* did not reach § 230; it only addressed whether the Taamneh Plaintiffs plausibly alleged violations of the ATA for purposes of Rule 12(b)(6). The *Taamneh* appeal is further limited by the fact that the Taamneh Plaintiffs only appealed the dismissal of their aiding-and-abetting claim.

The Taamneh Plaintiffs' aiding-and-abetting claim stems from Abdulkadir Masharipov's murder of Nawras Alassaf at the Reina nightclub on January 1, 2017. Masharipov's connection to ISIS is not disputed. He filmed his "martyrdom" video, wherein he stated that he was going to carry out a suicide attack in the name of ISIS, and requested that his son grow up to be a suicide bomber like him.[20] About one year before the Reina Attack, ISIS instructed Masharipov to move to Turkey with his family and await further orders. ISIS provided Masharipov with an assault rifle, ammunition, and stun grenades, and directed Masharipov when and where to attack. ISIS also sent Masharipov footage taken inside the Reina nightclub, and Masharipov viewed it at length to memorize the floor plan in preparation for his attack.

1

The Taamneh Plaintiffs' aiding-and-abetting claim is governed by the standards set forth in *Halberstam*. The first *Halberstam* element requires that "the party whom the

[20] The operative complaint alleges "[m]artyrdom videos, shared via Defendants' websites, are tools of propaganda frequently used by ISIS. These videos are used as psychological weapons in ISIS's attempt to establish validity for their actions, inspire fear in their enemies, or spread their ideology for political or religious ambitions."

defendant aids must perform a wrongful act that causes an injury." 705 F.2d at 477. The parties do not dispute that the Reina Attack was an "act of international terrorism" that was "committed, planned, or authorized" by ISIS. Nor do the parties dispute that the Reina Attack caused the Taamneh Plaintiffs' injury—the killing of Nawras Alassaf.

2

The second *Halberstam* element of aiding-abetting liability requires the defendant to be "generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance." *Id*. The Taamneh Plaintiffs also satisfied this element.

The Taamneh Plaintiffs allege that, at the time of the Reina Attack, defendants were generally aware that ISIS used defendants' platforms to recruit, raise funds, and spread propaganda in support of their terrorist activities. The FAC alleges that, despite "extensive media coverage" and legal and governmental pressure, defendants "continued to provide these resources and services to ISIS and its affiliates, refusing to actively identify ISIS's Twitter, Facebook, and YouTube accounts, and only reviewing accounts reported by other social media users." These allegations suggest the defendants, after years of media coverage and legal and government pressure concerning ISIS's use of their platforms, were generally aware they were playing an important role in ISIS's terrorism enterprise by providing access to their platforms and not taking aggressive measures to restrict ISIS-affiliated content. *See Linde*, 882 F.3d at 329; *see also Halberstam*, 705 F.2d at 477.

3

The third *Halberstam* element requires the plaintiff to allege the defendant knowingly and substantially assisted the principal violation. 705 F.2d at 477. We conclude the Taamneh Plaintiffs' complaint satisfied this element.

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.[21] First, the act

[21] Many of the allegations we discuss in the context of *Taamneh* were also raised in a similar form in the *Gonzalez* TAC. But because of the application of § 230 immunity in *Gonzalez*, we did not have occasion to consider them in our evaluation of the Gonzalez Plaintiffs' aiding-and-abetting claim.

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. *Fields*, 881 F.3d at 748.

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, *see Siegel*, 933 F.3d at 225, 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.

We are mindful that a defendant's state of mind is an important factor, and that the FAC alleges the defendants regularly removed ISIS-affiliated accounts and content. *See Halberstam*, 705 F.2d at 488 (noting that Hamilton's state of mind "assume[d] a special importance" because her knowing assistance evidenced "a deliberate long-term intention to participate in an ongoing illicit enterprise" and an "intent and desire to make the venture succeed"). But the Taamneh Plaintiffs also allege that defendants allowed ISIS accounts and content to remain public even after receiving complaints about ISIS's use of their platforms.

We also recognize the need for caution in imputing aiding-and-abetting liability in the context of an arms-length transactional relationship of the sort defendants have with

users of their platforms. Not every transaction with a designated terrorist organization will sufficiently state a claim for aiding-and-abetting liability under the ATA. But given the facts alleged here, we conclude the Taamneh Plaintiffs adequately state a claim for aiding-and-abetting liability.

VII

Finally, we turn to *Clayborn*. The claims in *Clayborn* arise from a fatal shooting in San Bernardino, California in which Sierra Clayborn, Tin Nguyen, and Nicholas Thalasinos lost their lives. The district court did not address § 230 immunity and the Clayborn Plaintiffs only appeal the dismissal of their ATA claim for aiding-and-abetting liability.

The Clayborn Plaintiffs allege that Google, Twitter, and Facebook provided key assistance to the two shooters, Farook and Malik. To plausibly allege an aiding-and-abetting claim under the ATA, the Clayborn Plaintiffs must allege that ISIS "committed, planned, or authorized" the San Bernardino Attack. 18 U.S.C. § 2333(d)(2); *see also Halberstam*, 705 F.2d at 477. The district court held the Clayborn Plaintiffs failed to plausibly allege that ISIS committed, authorized, or planned the San Bernardino Attack because the ties between the attack and ISIS were "insufficient to plausibly plead claims for indirect liability." The court interpreted § 2333(d)(2) to require "evidence that ISIS itself planned or carried out the attack," requiring more than allegations that ISIS sought to "generally radicalize" individuals and that ISIS promoted terrorist attacks.

On appeal, the Clayborn Plaintiffs argue three "central allegations" sufficiently connect ISIS to Farook and Malik: (1) ISIS claimed responsibility for the San Bernardino Attack

after the fact; (2) Malik pledged allegiance to then-ISIS leader Abu Bakr al-Baghdadi at some point during the attack; and (3) "the FBI confirmed evidence that Farook had face to face meetings a few years prior to the attack with five people the Bureau investigated and labeled [as] having 'links to terrorism.'" From these allegations, the Clayborn Plaintiffs urge us to infer "that ISIS authorized the San Bernardino shooting sometime before the attack."

We conclude the operative complaint does not plausibly allege that ISIS "committed, planned, or authorized" the San Bernardino Attack. It is undisputed that Farook and Malik planned and carried out the mass killing, but the Clayborn Plaintiffs' allegations suggest only that ISIS approved of the shooting *after* learning it had occurred, not that it authorized the attack beforehand. The allegations in the operative complaint indicate some connection between the shooters and ISIS is possible, but more is needed in order to plausibly allege a cognizable claim for aiding-and-abetting liability. *Twombly*, 550 U.S. at 555 ("Factual allegations must be enough to raise a right to relief above the speculative level . . . on the assumption that all of the complaint's allegations are true . . . ." (internal citation omitted)).

The Sixth Circuit decision in *Crosby* aligns with our conclusion. In *Crosby*, plaintiffs filed claims against Google, Twitter, and Facebook under the ATA following the mass shooting at the Pulse Night Club in Orlando, Florida. 621 F.3d at 619. The plaintiffs alleged "ISIS 'virtually recruited' people through online content, [the shooter] saw this content at some point before the shooting, and [the shooter] injured Plaintiffs." *Id.* at 626. The *Crosby* plaintiffs also alleged that ISIS took responsibility for the attack after the fact. *Id.* at 619. Even taking the allegations as true, the

Sixth Circuit concluded the complaint alleged the shooter was "self-radicalized" and never had any contact with ISIS, and failed to allege that ISIS gave permission for the attack. *Id.* Thus, the Sixth Circuit held "there [were] insufficient facts to allege that ISIS 'committed, planned, or authorized' the Pulse Night Club shooting." *Id.* at 626.

The dissent would hold that the Clayborn Plaintiffs adequately stated a claim for aiding and abetting liability. Specifically, the dissent relies on the Clayborn Plaintiffs' allegation that Farook and Malik used a tactic a Department of Justice report described as "a frequent, well documented practice in international terrorism incidents" that had been outlined in Al Qaeda and ISIS magazines disseminated on defendants' platforms. We disagree. Farook and Malik's use of well-known terrorist tactics do not give rise to an inference that their attack was "implicitly authorized" *by ISIS*.

The dissent urges us to apply common law principles of agency to conclude that ISIS authorized the San Bernardino Attack by ratifying it after the fact. We cannot agree this element is adequately alleged. Section 2333(d)(2) requires plaintiffs to demonstrate the act of international terrorism was "committed, planned, or authorized" by a foreign terrorist organization. The language Congress adopted gives no indication that the "committed, planned, or authorized" element is satisfied merely because a foreign terrorist organization praises an act of terrorism.

Even if Congress intended "authorized" to include acts ratified by terrorist organizations after the fact, ISIS's statement after the San Bernardino Attack fell short of ratification. The complaint alleges that ISIS stated, "Two followers of Islamic State attacked several days ago a center

in San Bernardino in California, we pray to God to accept them as Martyrs." This clearly alleges that ISIS found the San Bernardino Attack praiseworthy, but not that ISIS adopted Farook's and Malik's actions as its own. *See Restatement (Third) of Agency*, § 4.01 cmt. b, (1933) ("The act of ratification consists of an externally observable manifestation of assent to be bound by the prior act of another person.").

Because the Clayborn Plaintiffs' allegations do not plausibly allege that ISIS "committed, planned, or authorized" the San Bernardino Attack, the Clayborn Plaintiffs did not adequately state a claim for aiding and abetting an act of international terrorism under § 2333(d)(2). *See Crosby*, 921 F.3d at 626.[22]

VIII

The plaintiffs in these three cases suffered devastating losses from acts of extreme and senseless brutality, and their claims highlight an area where technology has dramatically outpaced congressional oversight. There is no indication the drafters of § 230 imagined the level of sophistication algorithms have achieved. Nor did they foresee the

[22] The district court did not reach whether the San Bernardino Attack was an "act of *international* terrorism." (emphasis added). This question appears to be much closer in *Clayborn* than either of the other appeals before us. *See* 18 U.S.C. § 2331(1)(C). In *Clayborn*, the attack was planned and executed in the United States by a U.S. citizen and his wife. Although the San Bernardino Attack was undoubtably an act of terror, it is less clear whether the complaint alleged sufficient international activity to qualify the San Bernardino Attack as an instance of "international terrorism." Having held the Clayborn Plaintiffs failed to state a claim for secondary liability on other grounds, we do not decide that question.

circumstance we now face, in which the use of powerful algorithms by social media websites can encourage, support, and expand terrorist networks. At the time § 230 was enacted, it was widely considered "*impossible* for service providers to screen each of their millions of postings for possible problems." *Carafano*, 339 F.3d at 1124 (emphasis added) (quoting *Zeran*, 129 F.3d at 330–31). But it is increasingly apparent that advances in machine-learning warrant revisiting that assumption. Indeed, social media companies are reportedly making laudable strides to develop tools to identify, flag, and remove inherently illegal content such as child pornography.[23] Section 230's sweeping immunity is likely premised on an antiquated understanding of the extent to which it is possible to screen content posted by third parties.

There is no question § 230(c)(1) shelters more activity than Congress envisioned it would. Whether social media companies should continue to enjoy immunity for the third-party content they publish, and whether their use of algorithms ought to be regulated, are pressing questions that Congress should address.

IX

With respect to *Gonzalez*, we affirm the district court's ruling that § 230 immunity bars the plaintiffs' non-revenue sharing claims. Separately, we conclude the TAC's direct liability revenue-sharing claims did not plausibly allege that Google's actions qualified as acts of international terrorism within the meaning of § 2331(1), and that the secondary liability revenue-sharing claims failed to plausibly allege

[23] *Supra* note 11.

either conspiracy or aiding-and-abetting liability under the ATA.

With respect to *Taamneh*, we reverse the district court's judgment that the FAC failed to adequately state a claim for secondary liability under the ATA.

With respect to *Clayborn*, we affirm the judgment of the district court that Clayborn Plaintiffs failed to state a claim for secondary liability under the ATA.[24]

The judgment in No. 18-16700 is **AFFIRMED.**

The judgment in No. 18-17192 is **REVERSED AND REMANDED.**

The judgment in No. 19-15043 is **AFFIRMED.**

[24] Amicus Electronic Frontier Foundation (EFF) moves to file an amicus brief in this appeal. We grant the motion, and grant the Gonzalez Plaintiffs' motion to file an oversized reply brief in order to respond to EFF. In its amicus brief, EFF raises several arguments concerning the First Amendment. We often "decline to consider" amicus briefs that seek "to raise issues not raised or briefed by the parties." *Am. Trucking Ass'ns, Inc. v. City of Los Angeles*, 559 F.3d 1046, 1053 n.11 (9th Cir. 2009) (citing *Day v. Apoliona*, 496 F.3d 1027, 1035 n.11 (9th Cir. 2007)). Here, because the parties did not raise the First Amendment, the panel declines to consider EFF's arguments on this issue.

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), *cert. denied*, 140 S. Ct. 2761 (2020), 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.

47 U.S.C. § 230(c)(1) provides: "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." "This grant of immunity applies only if the interactive computer service provider is not also an 'information content provider,' which is defined as someone who is 'responsible, in whole or in part, for the creation or development of' the offending content." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc) (quoting 47 U.S.C. § 230(f)(3)). Although the statute was enacted in response to the risk of liability for defamation, the language of the statute applies to any cause of action based on the publication or speaking of information content. *See Barnes*

v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009). This Court has held that immunity under section 230 extends to "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020) (quoting *Barnes*, 570 F.3d at 1100–01).

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. Dissent at 96–97. 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. *See Dyroff*, 934 F.3d at 1095. 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.

Nothing in the history of section 230 supports a reading of the statute so expansive as to reach these website-generated messages and functions. Section 230 "provide[d] internet companies with immunity from certain claims 'to promote the continued development of the Internet and other interactive computer services.'" *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 681 (9th Cir. 2019) (quoting 47 U.S.C. § 230(b)(1)). But as Judge Katzmann thoroughly explained in his dissent in *Force*, the aim of section 230 was to avoid government regulation of internet content while "empower[ing] interactive computer service providers to self-regulate, and . . . provid[ing] tools for parents to regulate, children's access to inappropriate material." *Force*, 934 F.3d at 79 (Katzmann, C.J., concurring in part and dissenting in part). A New York state court had just held that an Internet provider that hosted online bulletin boards could be held liable for defamation as a publisher because it actively monitored and removed offensive content. *See Batzel v. Smith*, 333 F.3d 1018, 1029 (9th Cir. 2003) (citing *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *4 (N.Y. Sup. Ct. May 24, 1995) (unpublished)). So section 230, responding to *Stratton Oakmont*, prevented providers from being treated as the publisher of third-party content, 47 U.S.C. § 230(c)(1), and eliminated liability for actions taken to restrict access to objectionable material, *id.* § 230(c)(2). Although "Congress grabbed a bazooka to swat the *Stratton-Oakmont* fly," *Force*, 934 F.3d at 80 (Katzmann, C.J., concurring in part and dissenting in part), still, neither the text nor the history of section 230 supports a reading of "publisher" that extends so far as to reach targeted, affirmative recommendations of content or of contacts by social media algorithms.

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.

Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, involved a social networking website that allowed users anonymously to share their experiences on any topic and post and answer questions. Importantly, the website, Experience Project, also "recommended groups for users to join, based on the content of their posts and other attributes, using machine-learning algorithms." *Id.* at 1095. One user, Wesley Greer, posted a question about buying drugs in a heroin-related group, and the website sent him a notification when a nearby drug dealer posted in the same group. *Id.* Greer bought heroin laced with fentanyl from the dealer and died from the drug. *Id.*

Dyroff held that "[b]y recommending user groups and sending email notifications, [the website] was acting as a publisher of others' content. These functions—recommendations and notifications—are tools meant to facilitate the communication and content of others. They are not content in and of themselves." *Id.* at 1098. To me, those two sentences actually illustrate why the recommendation and email notifications are *not* actions taken in the role of publisher. The activities highlighted *do* involve communication by the service provider, and so are activities independent of simply providing the public with content supplied by others.

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.

The problem in our case law goes considerably further back than *Dyroff*. Before *Dyroff*, *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, held that section 230 did not immunize a website that "induced third parties to express illegal preferences" by including discriminatory criteria in a required form for people setting up profiles, 521 F.3d at 1165. Roommates.com operated a website listing rentals and people seeking rooms and required subscribers to list information about their own and their preferred roommates' sex, sexuality, and family status. *Roommates* held that although the information itself was provided by third parties, the mandatory nature of the information and the "limited set of pre-populated answers" made Roommates.com into "much more than a passive transmitter of information provided by others; it becomes the

developer, at least in part, of that information." *Id.* at 1166. *Roommates* distinguished between "providing *neutral* tools [for users] to carry out what may be unlawful or illicit searches" or "allow[ing] users to specify whether they will or will not receive emails by means of *user-defined* criteria" and operating "in a manner that contributes to the alleged illegality." *Id.* at 1169.

As the majority discusses, Maj. Op. at 38, *Roommates* relied on our prior decision in *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003), which held that a dating website was not liable for an unauthorized and libelous profile created by a third party, *see id.* at 1122, 1125. The dating website "provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs." *Roommates*, 521 F.3d at 1172. *Carafano* determined that the website was being treated as a publisher and that the "additional features, such as 'matching' profiles with similar characteristics" were not sufficient to make the website into the "creator" or "developer" of the content in user profiles under 47 U.S.C. § 230(f)(3). 339 F.3d at 1125; *see id.* at 1124–25. Instead, the Court determined that such features were more akin to editing or selection. *Id.* at 1124. A tool matching two people who choose to share similar information about themselves is nearly identical to Facebook's algorithm suggesting possible connections and is similar to algorithms recommending new videos based on past user viewing habits, and to the recommendation and notification functions of the Experience Project at issue in *Dyroff*. *Dyroff* concluded that "[t]he [Experience Project's] recommendation and

notification functions," like the tools in *Carafano*, could not give rise to liability, because they "helped facilitate . . . user-to-user communication, but . . . did not materially contribute . . . to the alleged unlawfulness of the content," 934 F.3d at 1099.

The partial dissent considers the Gonzalez Plaintiffs' allegations "more akin to those in *Roommates.com* than *Dyroff* because of the unique threat posed by terrorism compounded by social media." Dissent at 99. But the subject matter of the third-party content does not dictate whether an interactive computer service is being treated as a publisher of that content. Nor does the test proposed in the partial dissent, which focuses on "message[s] designed to recruit individuals for a criminal purpose" and material contribution "to a centralized cause giving rise to a probability of grave harm," *id.* at 100, meaningfully distinguish our case law, particularly *Dyroff*. The sale of heroin is a criminal purpose, and many drug dealers operate as part of criminal networks. Although the harm caused by a terrorist attack is immense, the harm caused by the sale of fentanyl-laced heroin is certainly "grave"—it led to Greer's death in *Dyroff*. The allegation that the recommendation to users of illegal terrorist messages establishes the illegality of Google's actions under the Anti-Terrorism Act (ATA), 18 U.S.C. § 2333, exactly parallels the allegation in *Dyroff* that the dissemination of messages connecting drug dealers to buyers contributed to the harms Congress intended to combat by prohibiting drug trafficking.

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. As Judge Gould and Judge Katzmann both emphasize, algorithms on social media sites do not offer just one or two suggestions; they operate cumulatively and dominate the user experience. "The cumulative effect of recommend[ations] . . . envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own." *Force*, 934 F.3d at 83 (Katzmann, C.J., concurring in part and dissenting in part). If viewers start down a path of watching videos that the algorithms link to interest in terrorist content, their immersive universe can easily become one filled with ISIS propaganda and recruitment. Even if the algorithm is based on content-neutral factors, such as recommending videos most likely to keep the targeted viewers watching longer, the platform's recommendations of what to watch send a message to the user. And that message—"you may be interested in watching these videos or connecting to these people"—can radicalize users into extremist behavior and contribute to deadly terrorist attacks like these.

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

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

I

I concur in part in the majority opinion in its Parts I and II, Part III.A through III.D, Part III.F, and Part VI, but respectfully dissent in part as to Part III.E, and Parts IV, V, and VII. These cases involve several shooting or bombing incidents involving ISIS terrorists at far-flung worldwide locations of Paris, France; Istanbul, Turkey; and San Bernardino, California, in the United States. They also involve claims that Internet or social media companies such as Google, YouTube, Facebook, and Twitter contributed to acts of terrorism because of the operation of their procedures and platforms. I concur insofar as the majority would reverse in part the dismissal of revenue-sharing claims in *Gonzalez v. Google*, and insofar as it would reverse the district court's judgment in *Taamneh v. Twitter* that the complaint failed to adequately state a claim for secondary liability under the Anti-Terrorism Act ("ATA"). However, I respectfully dissent as to the majority's dismissal of the *Gonzalez* claims on grounds of Section 230 immunity, and of failure to state a claim for direct or secondary liability under the ATA, because of the majority's mistaken conclusion that there was no act of international terrorism, and I also would hold that the complaint adequately alleged that there was proximate cause supporting damages on those claims.

I further note that the majority here makes its dismissive rulings solely on the pleadings and with no discovery to illuminate Plaintiffs' well-plead factual contentions. Federal Rule of Civil Procedure 12(b)(6) permits dismissal of claims without pondering evidence in cases where a complaint fails to state a claim. FRCP 12(b)(6) has an important role to play in efficiently clearing the courts of suits that lack plausible allegations or where a legal barrier like preemption exists. Yet in a case that does not warrant such a prompt dismissal,[1] we do the legal system a disservice by dismissing a case before considering the evidence that can arise in a properly monitored discovery period. A defendant that actually has immunity is a good candidate for 12(b)(6) dismissal, but if the district court's conception of the scope of immunity is incorrect, as I believe it was here, then its dismissal under that rule will be untenable.

I would hold that Section 230 of the Communications Decency Act ("CDA") does not bar the Gonzalez Plaintiffs' claims for direct and secondary liability under the ATA, and I would allow those claims to proceed to the district court for a reasonable period for discovery. I agree that claims can proceed in the *Taamneh* case, and accordingly agree with reversing and remanding in that case. And on the *Clayborn*

[1] Doubtless the Defendant social media companies would benefit from 12(b)(6) dismissal at the outset—in a case where they are actually immune—to avoid expensive and time-consuming discovery procedures. However, while that relief would be "swift," it would not necessarily be just. I am reminded of the often-quoted observation by Justice Potter Stewart, when he was a U.S. Circuit Judge and before his elevation to the Supreme Court, that: "Swift justice demands more than just swiftness." *Henderson v. Bannan*, 256 F.2d 363, 385 (6th Cir. 1958) (Stewart, J., dissenting) (capitalization altered). This observation has currency in civil cases as well, and not only in the criminal justice context.

v. Twitter case, I respectfully dissent because I think that the majority's conception of an attack authorized by ISIS is inconsistent with the allegations of the operative complaint and well-established principles of tort and agency law. Further, on all these claims, I would permit amendment if sought by plaintiffs based on a theory that the claims are supported by specialized federal common law that may be applied in cases involving a particularly strong national interest and a gap in applicable statutory law.[2]

I further urge that regulation of social media companies would best be handled by the political branches of our government, the Congress and the Executive Branch, but that in the case of sustained inaction by them, the federal courts are able to provide a forum responding to injustices that need to be addressed by our justice system. Here, that means to me that the courts should be able to assess whether certain procedures and methods of the social media companies have created an unreasonably dangerous social media product that proximately caused damages, and here, the death of many.

The issues here cannot be considered without contemplating the specific facts alleged in the operative

[2] We do not ordinarily consider an issue that was not raised in the district court, *e.g.*, *Am. President Lines Ltd. v. Int'l Longshore & Warehouse Union, Alaska Longshore Div., Unit 60*, 721 F.3d 1147, 1157 (9th Cir. 2013), and similarly do not normally consider issues that are not presented to us in the briefing, *e.g.*, *United States v. Garcia*, 149 F.3d 1008, 1010 (9th Cir. 1998). However, these rules have exceptions that are applied by us in extraordinary cases where permitting such an issue to be considered is necessary to avoid a miscarriage of justice. *See Hormel v. Helvering*, 312 U.S. 552, 557 (1941). Here, the three complaints involve sufficiently strong interests of the families with loved ones lost to the ISIS attacks, so that these cases fall within the exception to the rule.

complaints. Because the treatment by the majority of the facts of the three cases captioned above is not contested by me, I mention only the briefest thumbnail sketch of what is involved in the three cases that are now on appeal:

Gonzalez v. Google, 18-16700, involved an ISIS shooting in Paris on November 13, 2015, which took the life of Nohemi Gonzalez, a 26-year-old U.S. citizen. This shooting was one among a broader series of ISIS attacks in Paris on the same day, including several suicide bombings and mass shootings.

Taamneh v. Twitter, 18-17192, concerns the notorious January 1, 2017 mass shooting by an ISIS operative at the Reina nightclub in Istanbul, Turkey, which left 39 people dead, 69 others injured, and resulted in the death of Nawras Alassaf.

Clayborn v. Twitter, 19-15043, concerns the December 2, 2015 attack by ISIS supporters at the Inland Regional Center in San Bernardino, California, which left 14 people dead and 22 others injured.

All of these terrorist incidents involved ISIS's supporters. In all three cases, Plaintiffs alleged that Google, through YouTube, and Twitter and Facebook, through their features, provided material support to international terrorism and aided and abetted international terrorism in violation of the ATA, as amended in 2016 by the Justice Against Sponsors of Terrorism Act ("JASTA"). I would hold that the challenged conduct of the social media companies is not immunized by Section 230 and that the complaints' allegations are sufficient to plausibly allege that the Defendant social media companies violated positive statutory law and proximately caused

damages to Plaintiffs. In addition, I would hold that the same types of claims can permissibly be asserted as a matter of federal common law upon amendment of the complaints. *See infra*, Section V.

II

My colleagues hold that Section 230 immunizes Google from the Gonzalez Plaintiffs' claims that the YouTube platform's content-generating algorithms aid and abet international terrorism by repeatedly recommending the propaganda videos of ISIS to users and by broadly disseminating violent and radicalizing terrorist messages.[3] It is true that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any

[3] The problem I challenge is not that the social media companies republish harmful propaganda from ISIS; the problem is the algorithms devised by these companies to keep eyes focused on their websites. Historian Anne Applebaum, who has evaluated the stresses on democracies in several countries in light of modern communications and technology, notes the following: "[S]ocial media algorithms themselves encourage false perceptions of the world. People click on the news they want to hear; Facebook, YouTube, and Google then show them more of whatever it is that they already favor, whether it is a certain brand of soap or a particular form of politics. The algorithms radicalize those who use them too. If you click on perfectly legitimate anti-immigration YouTube sites, for example, these can lead you quickly, in just a few more clicks, to white nationalist sites and then to violent xenophobic sites. Because they have been designed to keep you online, the algorithms also favor emotions, especially anger and fear. And because the sites are addictive, they affect people in ways they don't expect. Anger becomes a habit. Divisiveness becomes normal. Even if social media is not yet the primary news source for all Americans, it already helps shape how politicians and journalists interpret the world and portray it. Polarization has moved from the online world into reality." *See* Anne Applebaum, *Twilight of Democracy—The Seductive Lure of Authoritarianism* (1st ed. 2020).

information provided by another information content provider." 47 U.S.C. § 230(c)(1). But in my view, Section 230 was not intended to immunize, nor does its literal language suggest that it immunizes, companies providing interactive computer services from liability for serious harms knowingly caused by their conduct. Plaintiffs raise a genuine factual issue of whether Defendants knew that ISIS and its supporters were inserting propaganda videos into their platforms, which permits the inference that these social media companies were aware of the risks to the public from incipient terrorists who, inflamed by ISIS videos, would wreak havoc upon "infidels" who might be encountered by them.

Even if under Section 230 Google should not be considered the publisher or speaker of propaganda messages posted by ISIS or its sympathizers, the YouTube platform nonetheless magnified and amplified those communications, joining them with similar messages, in a way that contributed to the ISIS terrorists' message beyond what would be done by considering them alone. Because ISIS depended on recruits to carry out its campaign of worldwide hatred and violence, disseminating its terrorist messages through its propaganda videos was a proximate cause of the terrorist attacks at issue here. When fairly read with notice pleading principles in mind, the complaints plausibly allege ISIS's dependence on recruitment through social media's free publicity and vast network.

I do not believe that Section 230 was ever intended to immunize such claims for the reasons stated in Chief Judge Katzmann's cogent and well-reasoned opinion concurring in part and dissenting in part in *Force v. Facebook, Inc.*, 934 F.3d 53, 76–89 (2d Cir. 2019). Chief Judge Katzmann's

partially dissenting opinion in *Force v. Facebook* is appended as Attachment A to this partial dissent. Although I substantially agree with Judge Katzmann's reasoning regarding Section 230 immunity, I add some thoughts of my own. In short, I do not believe that Section 230 wholly immunizes a social media company's role as a channel of communication for terrorists in their recruiting campaigns and as an intensifier of the violent and hatred-filled messages they convey. The law should not give social media platforms total immunity, and in my view it does not, because the conduct plausibly alleged does have "some direct relationship," *Fields v. Twitter, Inc.*, 881 F.3d 739, 744 (9th Cir. 2018), between the asserted injuries of the Plaintiff families and the Defendant social media companies' conduct. Further, Plaintiffs plausibly alleged aiding and abetting claims because providing the channels of communication for inflammatory videos should be considered substantial assistance to the primary violations of terrorist shootings or bombings.

The majority splits Plaintiffs' claims into two categories: claims based on Google's content-generating algorithms (the "non-revenue sharing claims"), and claims based on ISIS's use of Google's advertising program, AdSense (the "revenue sharing claims"). 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 viewer 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.

Section 230 of the CDA was aimed at giving Internet companies some breathing space to permit rapid growth of them and the economy by providing that when information was posted on a website, the interactive computer service hosting that website would not be liable for the substance of the content posted by the user. Pub. L. 104-104, § 509, 110 Stat. 56, 56, 137–39; *Reno v. ACLU*, 521 U.S. 844, 857–58 (1997). Our circuit has developed and consistently applied a three-part test, the *Barnes* factors, for when immunity applies. *See Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019). Under those factors, a defendant is entitled to Section 230 immunity when: (1) the defendant is "a provider or user of an interactive computer service, (2) whom the plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker," (3) "of information provided by another information content provider." *Id.* at 1097 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009)).

The factor at issue here is the second. 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. Here, Plaintiffs allege that Google's "Services" include not just publishing content, but also "use of Google's infrastructure, network, applications, tools and features, communications services," and other

specialized tools like "Social Plugins" and "Badges." Similar allegations are made about other platforms' tools and procedures. 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 believe that my view is consistent with our decision in *Dyroff*. The majority relies on *Dyroff* for the proposition that Google's algorithms, which recommend ISIS content to users, are "neutral tools" meant to facilitate communication and the content of others. According to my colleagues, then, under Section 230, Google does not transcend the role of a publisher by merely recommending terrorism-related content based on past content viewed.

In *Dyroff*, Plaintiff challenged a social networking website called "Experience Project," which allowed users to anonymously share their first-person experiences, post and answer questions, and interact with other users about different topics. 934 F.3d at 1094. The website interface "did not limit or promote the types of experiences users shared"—instead, it was up to the user to use the site's "blank box" approach to generate content. *Id.* The site also used machine-learning algorithms to recommend groups for users to join based on the content of their posts. *Id.* at 1095. Plaintiff alleged that the site's functions, including recommendations of new groups and notifications from groups of which the user is a member, facilitated an illegal drug sale that resulted in the death of Plaintiff's son, Wesley Greer. *Id.* Greer posted on the site asking about where to

find heroin in a particular city, and a fellow user responded and sold fentanyl-laced heroin to Greer. *Id.* Greer was sent an email notification when the other user posted, which resulted in the drug transaction. *Id.* We held that the site was entitled to Section 230 immunity because Plaintiff sought to treat the defendant as the publisher of Greer and his dealer's content. *Id.* at 1097.

We distinguished the facts in *Dyroff* from *Fair Housing Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1167–69 (9th Cir. 2008) (*en banc*). In *Roommates*, we held that Section 230 did not immunize a website that matched people renting rooms with people looking for somewhere to live from liability under federal and state housing anti-discrimination laws. *Id.* at 1161–62. The Roommates.com website design guided users through required discriminatory criteria, "inducing third parties to express illegal preferences," *id.* at 1165, and therefore the website itself "directly participate[d] in developing the alleged illegality." *Dyroff*, 934 F.3d at 1099. In *Dyroff*, then, we drew a distinction between true material contribution to a third party's content—which would involve "responsibility for what makes the displayed content illegal or actionable"—and "actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content." *Id.* (quoting *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 n.4 (9th Cir. 2016) (citation omitted)).

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 "[t]he 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.[4] 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]

---

[4] The Counter Extremism Project, White Paper, *The eGlyph Web Crawler: ISIS Content on YouTube* (July 2018), https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf.

[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

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 provid[ed] 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.[6]

---

companies could not police and prohibit the transmission of violent ISIS propaganda videos, in the periods preceding a terrorist attack. *See* Kate Conger & Mike Isaac, *Twitter Permanently Bans Trump, Capping Online Revolt*, N.Y. TIMES (Jan. 8, 2021), https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html.

[6] The majority contends that my view, which considers the danger inherent in the message amplified by Google, is inconsistent with congressional intent in enacting Section 230(c)(1). Though it is true that an interactive computer service is immune when it is "treated as the publisher or speaker of *any information* provided by another information content provider," 47 U.S.C. § 230(c)(1) (emphasis added), the same portion of the statute makes clear that for Section 230 to apply, the

Plaintiffs' allegations underscore the danger of amplifying ISIS's recruiting messages. Plaintiffs allege that ISIS has used YouTube "to cultivate and maintain an image of brutality, to instill greater fear and intimidation," and to distribute videos "made in anticipation of the [Paris] attack showing each of the ISIS terrorists who carried out the attacks telling of their intentions and then executing a captive for the camera." Plaintiffs allege that ISIS "not only uses YouTube for recruiting, planning, inciting, and giving instructions for terror attacks," but also uses it "to issue terroristic threats . . . intimidate and coerce civilian populations, take credit for terror attacks, communicate its desired messages about the terror attacks . . . [and] demand and attempt to obtain results from the terror attacks."

I note that Chief Judge Katzmann's concurrence in part and dissent in part in *Force v. Facebook, Inc.*, 934 F.3d 53, 76–89 (2d Cir. 2019), relied on a reading of *Roommates.com* that is consistent with my view here. Chief Judge Katzmann contended that Facebook is developing content by actively providing friend suggestions between users who have expressed similar interests—in other words, the algorithms provided a "message" from Facebook to the user. *Id.*

---

plaintiffs must be attempting through their suit to treat the website as a publisher or speaker. But emphasizing the danger of the terrorist message shows that because Google is amplifying ISIS's recruitment message—and thus acting as a content generator, not merely a publisher—the inherent danger of dissemination materially contributes to the illegality of the conduct. *See Roommates*, 521 F.3d at 1168. If a website is acting as a publisher, then under Section 230 it will be immune no matter what information it publishes from another source. But if, as is the case here, the dangerous nature of the message makes amplifying that message transform what would otherwise be mere publishing into content development, then the website is no longer immune under Section 230.

at 82–83. In the same way, YouTube is "proactively creating networks of people," *id.* at 83, who are sympathetic to the ISIS cause, and Google is delivering the message that those YouTube users may be interested in contributing to ISIS in a more tangible way.

Furthermore, propagating ISIS messages has an amplification effect that is greater than the sum of each individual connection. *See Force*, 934 F.3d at 83 (Katzmann, J., dissenting in part) ("The cumulative effect of recommending several friends, or several groups or events, has an impact greater than the sum of each suggestion. It envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own."). Plaintiffs allege that Google does so in part by "us[ing] 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.[7] With each person that joins its ranks, ISIS grows in power and resources. It is the fact of recruitment to

[7] As the Counter Extremism Project observes, "there is a clear link between extremist videos and individuals who have sought to support or join ISIS. A joint study from the University of Chicago's Project on Security and Threats and the Australian Strategic Policy Institute's Counter-Terrorism Policy Center found that 83% of Americans who committed or were charged with ISIS-related crimes between March 2014 and August 2016 watched ISIS propaganda videos." *See* White Paper, *eGlyph* at 2 (citing Robert Pape, et al., "The American Face of ISIS," Australian Strategic Policy Institute (Feb. 2017), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI_CPOST_ISIS_Indictees.pdf?2Tbn8TshXmujb1ft8f7PIR7sukzyr hka).

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. *See Force*, 934 F.3d at 83–84 (Katzmann, J., dissenting in part) (noting that "ATA torts are atypical" because the Act premises liability "not on publishing *qua* publishing, but rather on Facebook's provision of services and personnel to Hamas").

For the foregoing reasons, I would hold that Section 230 does not immunize Google from liability for its content-generating algorithms insofar as they develop a message to ISIS-interested users. The same reason supports lack of immunity for the other Defendant social media companies' use of their own algorithms, procedures, users, friends, or other means to deliver similar content from ISIS to the users of the social media. But even if *Dyroff* cannot be fairly distinguished, then our circuit should take this case *en banc* to modify or clarify the rule that machine-learning algorithms can never produce content within the meaning of Section 230,[8] or the Supreme Court should take up the proper

[8] The majority distinguishes Chief Judge Katzmann's dissent in *Force* in part by emphasizing that "Ninth Circuit case law forecloses his argument," though it recognizes that the *Force* dissent maintains that Section 230(c)(1) "need not be interpreted to immunize websites' friend-and-content-suggestion algorithms."

interpretation of Section 230 and bring its wisdom and learning to bear on this complex and difficult topic.[9]

III

Having determined that Section 230 does not immunize Google for liability for either set of claims (non-revenue

---

I disagree that our case law must be read to foreclose the Gonzalez Plaintiffs' argument, but the majority's apparent recognition that friend-and-content-suggestion algorithms could fairly be interpreted as outside of Section 230's ambit lends support to a potential *en banc* call in this case.

[9] Recently, Justice Thomas commented in connection with the denial of a writ of certiorari in *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*, 141 S. Ct. 13 (2020), that the Court would soon find it appropriate to take up a case interpreting Section 230. Justice Thomas notes that a new look at the statute is warranted because "[w]hen Congress enacted the statute, most of today's major Internet platforms did not exist." *Id.* at 13 (Thomas, J., writing separately). Despite this, "many courts have construed the law broadly to confer sweeping immunity on some of the largest companies in the world." *Id.* Justice Thomas goes on to explain that courts' views of Section 230 have gone from a "modest understanding" to beyond what plausibly could have been intended by Congress, including conferring immunity "even when a company distributes content that it *knows* is illegal. *Id.* at 15 (emphasis in original). In this separate statement, Justice Thomas made clear his view that the scope of Section 230 immunity should be narrowed in line with congressional intent. I agree with Justice Thomas that Section 230 has mutated beyond the specific legal backdrop from which it developed, and I cannot join a majority opinion that seeks to extend this sweeping immunity further. When one considers the analysis in the statement of Justice Thomas in *Malwarebytes*, the dissent of Chief Judge Katzmann in *Force v. Facebook*, and the concurring opinion of Judge Tymkovich in *FTC v. Accusearch*, 570 F.3d 1187 (10th Cir. 2009), I believe that there is a rising chorus of judicial voices cautioning against an overbroad reading of the scope of Section 230 immunity.

sharing and revenue sharing), I next consider whether Plaintiffs properly stated a claim for direct liability under the ATA.

The majority holds that Section 230 immunizes Google from liability for Plaintiffs' non-revenue sharing claims, so it does not address whether Plaintiffs adequately alleged primary liability for those claims. Having held that Section 230 does not preclude it from considering that issue for the revenue sharing claims, however, the majority concludes that Plaintiffs still do not state a claim for primary liability under that theory. Specifically, my colleagues would decide that Plaintiffs fail to plausibly allege that Google committed an act of international terrorism, or that Google's actions proximately caused Nohemi Gonzalez's death. I address both bases for the majority's conclusion in turn.

A

I would hold that the Plaintiffs plausibly stated a claim that Google could be held primarily liable under the ATA based on both Google's revenue-sharing procedure and Google's content-generating algorithms. At the motion to dismiss stage, we accept all factual allegations in the complaint as true and construe them in the light most favorable to the nonmoving party. *Campidoglio LLC v. Wells Fargo & Co.*, 870 F.3d 963, 970 (9th Cir. 2017) (citation omitted).

The civil remedies provision of the ATA, 18 U.S.C. § 2333(a), allows a United States national who is a victim of "an act of international terrorism" to sue for damages in federal court. Acts constituting international terrorism "involve violent acts or acts dangerous to human life that are

a violation of the criminal laws of the United States or of any State . . . ." 18 U.S.C. § 2331(1)(A). Such acts must "appear to be intended . . . (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping." *Id.* § 2331(1)(B).

1

The majority acknowledges that Section 230 does not shield Google from liability on the revenue sharing claims because the allegations are "premised on Google providing ISIS with material support by *giving ISIS money*." I concur with that aspect of the opinion, but I would also add that providing monetary support to a foreign terrorist organization, with the constructive knowledge that that money would likely be used as part of the terrorist enterprise, qualifies as an "act of international terrorism." 18 U.S.C. § 2333(a).

I begin with the contours of Plaintiffs' revenue sharing claim. The complaint alleges that Google is aware of ISIS's presence on YouTube because it has received complaints about ISIS content, and it has "suspended or blocked selected ISIS-related accounts at various times." Plaintiffs also allege that Google shares a percentage of the revenue it generates from pairing advertisements and videos with the video poster. Through Google's commercial service, AdSense, users can register their accounts for "monetization." Plaintiffs allege that ISIS uses the AdSense monetization program to earn revenue. Before the YouTube video can be approved for advertisements, Google must review and approve the video. Google has therefore "reviewed and approved ISIS videos,

including videos posted by ISIS-affiliated users, for 'monetization' through Google's placement of ads in connection with those videos." Through those approvals, Google gains constructive knowledge of the fact that it provided financial support to ISIS and incentivized ISIS to continue to post videos on YouTube. Plaintiffs' allegations about Google's knowledge is bolstered by contentions that various news outlets reported on the kind of ads appearing before ISIS YouTube videos.

The majority mistakenly concludes that Google's conduct could not qualify as international terrorism because it is not "intended to intimidate or coerce a civilian population or to influence or affect a government." I disagree. The standard for intent under the ATA is not subjective; rather, it is a "matter of external appearance." *Boim v. Holy Land Found. for Relief & Dev.*, 549 F.3d 685, 694 (7th Cir. 2008) (*en banc*). I would hold that, on the facts alleged, a knowing provision of resources to a terrorist organization constitutes aid to international terrorism because an entity like Google appears to intend the natural and foreseeable consequences of its actions. *See Restatement (Second) of Torts*, § 8A (1965).

The majority relies on *Linde v. Arab Bank, PLC*, 882 F.3d 314 (2d Cir. 2018), to conclude that knowingly providing material support to a terrorist organization is not "an act of international terrorism" if it is motivated by economics. Besides the fact that *Linde* is a sister circuit decision that is not binding on our court, its facts and holding are also distinguishable. In *Linde*, the court expressly held that it was error for the district court to instruct the jury that proof that Arab Bank provided material support to a designated foreign terrorist organization, in violation of § 2339B, "necessarily proved the bank's commission of an act of international

terrorism." *Id.* at 325. Thus, the Second Circuit held only that violating § 2339B does not *inherently* create an act of terrorism. The court's reasoning continually references the context of its decision: whether it could find that the jury instruction error was harmless. *Id.* at 327 (holding that "the mere provision of routine banking services to organizations and individuals said to be affiliated with terrorists does not *necessarily* establish causation") (internal quotation marks and citation omitted) (emphasis added). Indeed, the court did not even decide whether Arab Bank's financial services to Hamas should be viewed as "routine" under the court's precedent, because that issue raised a question of fact for the jury to decide. *Id.*

Even accepting that providing material aid "does not invariably equate" to an act of international terrorism under § 2331(1), *Linde*, 883 F.3d at 326, there are clearly situations where providing such aid operates to endanger human life and manifests an apparent intent to coerce or intimidate civilians or to influence or affect governments. The Seventh Circuit's *Boim* decision represents such a case, despite the majority incorrectly characterizing Plaintiffs' reliance on it as "misplaced." In *Boim*, the court held that a jury could find defendants liable under the ATA when they had donated money to Hamas and Hamas-affiliated charities, knowing that Hamas used such money to finance violence towards at least some American citizens. 549 F.3d at 690. Because donating money to Hamas was like "giving a loaded gun to a child," it did not matter that the act of giving money is not a violent act itself because, in context, it would be "dangerous to human life." *Id.* (citation omitted). The Seventh Circuit recognized that imposing liability for providing money to a terrorist group "makes good sense as a counterterrorism measure," because "[d]amages are a less effective remedy against

terrorists and their organizations than against their financial angels." *Id.*

Boim relied on the foreseeability of the consequences of donating to Hamas to support its sensible holding that the donations would appear to be intended to intimidate or coerce a civilian population. *Id.* at 694; *see also Linde*, 883 F.3d at 327 (discussing *Boim*'s reasoning and stating that "given such foreseeable consequences," the donations met the statutory definition for an act of terrorism). The court analogized donating to a terrorist organization to giving a small child a loaded gun because in both cases, the actor is "doing something extremely dangerous and without justification." *Id.* at 693. "If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result." *Id.* (quoting *Restatement (Second) of Torts*, § 8A (1965)). The fact that the actor was not motivated by a desire for the child to shoot anyone is of no matter to the tort inquiry. *Id.*

The Gonzalez Plaintiffs allege that Google knew ISIS was using its AdSense program, and that therefore Google knew it was providing material support to a terrorist organization. The fact that Google was not motivated by a desire to augment ISIS's efforts to recruit other terrorists is irrelevant. The majority's argument—that Google's interactions with ISIS via revenue sharing are not intended to intimidate or coerce civilian populations because Google was "motivated by economics"—is an arbitrary line divorced from Section 2333's text and established principles of tort law. *Boim*—a decision properly based upon Section 2333's text and history—does not attempt to draw a line based on motivation. In fact, it rejects such a line as irrelevant to the question of

intent because a person intends what he knows is substantially certain to result from his act. 549 F.3d at 693. My colleagues attempt to distinguish *Boim* by noting that a donor to Hamas would likely share that organization's vision and objectives, but *Boim* did not rely on that aspect of targeted donation. Instead, the Seventh Circuit reasoned that "[a] knowing donor to Hamas" is "a donor who *knew* the aims and activities of the organization." *Id.* at 693–94 (emphasis added). It was the donor's *knowledge* of Hamas' activities, rather than his approval of it, that gave rise to liability.

2

Because amplifying ISIS's message and creating new networks of prospective terrorist recruits foreseeably provides material support to a terrorist organization, I would likewise hold that the complaint in *Gonzalez v. Google* states a claim that Google is primarily liable on a non-revenue sharing theory.

Terrorism is, in part, psychological warfare. The record shows that for ISIS terrorism is a psychological weapon. ISIS's most potent and far-reaching weapon is the Internet. The *Gonzalez* complaint alleges that "Google's YouTube platform has played an essential role in the rise of ISIS," which has become one of the largest perpetrators of violence in the world. ISIS uses YouTube to recruit members, plan terrorist attacks, issue threats, take credit for attacks, and demand and attempt to obtain results from the attacks by influencing government policies and conduct. While one of ISIS's goals is to commit acts of violence, "the physical attack itself and the harm to the individual victims of the attack" is just one piece of the puzzle—ISIS also uses terror

attacks as a means to communicate its political message and instill fear in those it considers its combatants. Thus, the impact of ISIS's terrorism is dependent upon its ability to communicate its message and reach its intended audiences. *Id.* Plaintiffs allege that "ISIS's use of violence and threats of violence [are] part of its program of terrorism, designed . . . to gain attention, instill fear and 'terror' in others, send a message, and obtain results." Because the communication of ISIS violence and threats is part of the terrorist attack, repeated postings and encouraged viewings of ISIS videos, as effected by Google's algorithms, is also part of the attack.

When a terrorist group blows up or shoots up or carves up passengers on an airplane, railroad car or a subway car, they do not do it merely to destroy property or injure people involved in those bombings, shootings, and knifing attacks. Instead, they aim to create fear in the public so that people will be afraid to use airplanes or railroad cars or subways or any general public area to go about their business as usual. Publicizing the event is just as essential to terrorists' success as is the bombing, shooting, or knifing itself. So-called "neutral" algorithms created by Facebook, Twitter, and Google, are then transformed into deadly missiles of destruction by ISIS, even though they were not initially intended to be used that way. But once there is a consistent stream of conduct by ISIS, it should be understood that defendants who passively ignore that conduct can be held to have intended the natural and probable consequences of their actions. *See Restatement (Second) of Torts*, § 8A (1965).

Just as sharing revenue with ISIS is "dangerous to human life," *Boim*, 549 F.3d at 690 (citation omitted), so is amplifying its message and encouraging recruitment to its ranks. Perhaps even more so because unlike money, which

is fungible, YouTube has a virtual monopoly on hosting extremist videos.[10] ISIS can get operating funds from a variety of sources, but very few platforms have the international network and infrastructure to which YouTube has access. Imposing liability on social media platforms for affirmatively amplifying ISIS's message can therefore "cut the terrorists' lifeline." *See id.* at 691.

B

Direct liability claims under the ATA require that plaintiffs show they suffered injury "by reason of an act of international terrorism." 18 U.S.C. § 2333(a). The "by reason of" phrasing has been understood to impose a requirement of proximate causation. *See, e.g.*, *Fields v. Twitter*, 881 F.3d 739, 744 (9th Cir. 2018). To meet this requirement, "a plaintiff must show at least some direct relationship between the injuries that he or she suffered and the defendant's acts." *Id.* at 744.

On my view of the case, the proximate cause issue must be reached, and I believe that it is satisfied. The ATA's purpose in part is to provide a financial remedy to victims of terrorism. Indeed, ATA's legislative history demonstrates Congress's intent to authorize the "imposition of liability at any point along the causal chain of terrorism." S. Rep. No. 102-342, at 22 (1992) (referencing "the flow of money" to terrorist groups).

[10] *See, e.g.*, Neima Jahromi, *The Fight for the Future of YouTube*, NEW YORKER (July 8, 2019), https://www.newyorker.com/tech/annals-of-technology/the-fight-for-the-future-of-youtube.

My view is consistent with our decision in *Fields v. Twitter*. In *Fields*, we acknowledged that acts of international terrorism are foreseeable consequences of financial support to a terrorist organization, but we also noted that such fungibility "does not relieve claimants of their burden to show causation." *Id.* at 749. *Fields* requires that a plaintiff plausibly allege a "direct relationship between a defendant's act and [a plaintiff's] injur[ies]," *id.* at 748, and that element is met here because there is a sufficient nexus.

Plaintiffs allege that ISIS operatives *involved in the Paris Attacks* posted links to ISIS YouTube videos. The sum of Plaintiffs' allegations demonstrate that the terrorists responsible for Plaintiffs' injuries used YouTube as an integral component of recruiting, and that such recruiting is necessary to carry out attacks at the scale of those in Paris.

Specifically, Plaintiffs allege that at least two of the twelve ISIS terrorists who carried out the Paris Attacks, Abaaoud and Laachraoui, used online social media platforms to post links to ISIS recruitment YouTube videos and "*jihadi* YouTube videos." Plaintiffs allege that Abaaoud, "considered the operational leader of the Paris Attack," was an active user of social media, including YouTube. In a March 2014 ISIS YouTube video, "Abaaoud gave a monologue (in French) recruiting *jihadi* fighters for ISIS."

Plaintiffs also allege that at the time of the attacks these two ISIS terrorists, who were "instrumental in the Paris Attack," were members of or at least involved with ISIS networks in Belgium called "The Zerkani Network" and Sharia4Belgium. The Belgian networks "used and relied on social media to build and maintain connections with ISIS recruits." Plaintiffs allege that there was a pervasive network

of ISIS recruiters in Belgium, which has been called "the epicenter of the Islamic State's efforts to attack Europe." Sharia4Belgium maintained several active YouTube channels, still active at the time of the Paris Attacks, "which it used to post sermons, speeches, news events, and other materials to lure, recruit, and indoctrinate young Muslims to travel to Syria and Iraq to join ISIS." Plaintiffs allege that there was significant overlap and coordination over time between Sharia4Belgium and "The Zerkani Network." Plaintiffs allege that Laachraoui was involved with Sharia4Belgium at the time of the Paris Attacks, and his social media accounts appear to show that he followed ISIS social media and posted links to *jihadi* YouTube videos on his own account.

Though Plaintiffs do not specifically allege how the perpetrators of the Paris Attack were radicalized, such an allegation is not necessary to plausibly state their claim. It is enough that the complaint alleged that the perpetrators themselves actively used YouTube to recruit others to ISIS, gaining resources with which to plan and implement their attacks; absent the participation of the social media companies for their own profit-centered purposes, terrorist groups like ISIS would not have these resources. Additionally, Plaintiffs alleged that "The Zerkani Network" recruited one of the shooters, Abaaoud, "an active user of social media, including YouTube," and also alleged that the network "used and relied on social media" to recruit, permitting the inference that it is probable Abbaoud was radicalized through social media. Viewing these allegations in the light most favorable to the nonmoving party, as we must, *Campidoglio*, 870 F.3d at 970, Plaintiffs have plausibly alleged a sufficient nexus between Google's conduct and the

Paris Attack victims' injuries to satisfy a proximate cause threshold standard.[11]

A possible analogy may help to illustrate how the social media companies' enhancement and spread of ISIS propaganda promoting violence and seeking to convert recruits has a direct relation to the damages caused here. Let's assume that a person on one side of a crowded football stadium fires a high-powered rifle aimed at a crowd on the opposite side of the stadium, filled with people, though all identities are unclear. Would the majority here say that the rifle shot striking an unidentified viewer on the other side of the stadium had no "direct relation" to the shooter and that the shot did not proximately cause a resulting death? I think not. There is direct relation between shooter and victim there sufficient to satisfy *Fields* and there is similar direct relation here between the challenged conduct of the Defendant social media companies and the victims of ISIS violence in these cases to say that the challenged conduct, if shown to be illegal, was a proximate cause of damages.

---

[11] It is worth noting that the contrary conclusion, espoused by the majority, would put these and future plaintiffs in an untenable position. If we required plaintiffs to specify exactly how an individual terrorist became radicalized without the benefit of discovery, then it is unlikely that any such claims could go forward. At the motion to dismiss stage, with notice pleading principles in mind, the Gonzalez Plaintiffs need only plausibly allege "some direct relation" between the terrorist's actions and the social media companies' conduct. *See Fields*, 881 F.3d at 749 (citation omitted). Here, Plaintiffs alleged that the perpetrator of the Paris Attack was a member of a particular network that used social media to recruit its members, and that the perpetrator himself was a regular user of social media. Given that it is unlikely potential terrorists will announce the avenues by which they were radicalized, such inferences are permissible.

IV

I next turn to whether Plaintiffs have adequately alleged claims against Google for secondary liability under JASTA. As with primary liability, the majority addressed only the revenue sharing claims in its opinion, but I would hold that for either set of claims, Plaintiffs have successfully stated a claim for secondary liability.

Congress amended the ATA by enacting JASTA in 2016, Pub. L. No. 144-222, 130 Stat. 854 (Sept. 28, 2016), which extends liability to persons who aid and abet by providing substantial assistance to persons who commit acts of international terrorism, and those who conspire to commit such acts. 18 U.S.C. § 2333(d)(2). 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." *Id*. I recognize the proper legal framework for analyzing such claims as that described in *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983). Like the majority, I first conclude that the first two *Halberstam* factors have been satisfied here: (1) the party whom the defendant aids performed a wrongful act that caused an injury; and (2) the defendant was "generally aware of his role as part of an overall illegal or tortious activity at the time that he provide[d] the assistance." *Halberstam*, 705 F.2d at 477. For the first element, the complaint plausibly alleges that the Paris Attacks were "committed, planned, or authorized" by ISIS, a designated terrorist organization. *See* 18 U.S.C. § 2333(d)(2). For the second element, I agree that Google was "generally aware of its role in ISIS's terrorist activities" at the time it used its content-generating algorithms to send a message to YouTube users and at the time it shared revenue

through AdSense. In both cases, Google was aware that it assumed a role in ISIS's terrorist activities. *See Halberstam*, 705 F.2d at 488; *see also Linde*, 882 F.3d at 329 (noting that the element does not require a showing of "specific intent" as in criminal aiding and abetting, nor does it require that the defendant "knew of the specific attacks at issue").

Unlike my colleagues, however, I also conclude that the final element is met: the defendant "knowingly and substantially assisted[ed] the principal violation." *Halberstam*, 705 F.2d at 488. The majority acknowledges that Google knowingly assisted the principal violation, but denies that such assistance was "substantial."[12]

I would hold that Google's assistance via its content-generating algorithms and revenue sharing was both knowing and substantial. I need not view the non-revenue sharing claims and revenue sharing claims in isolation in this portion of my analysis. Because I conclude that both sets of Plaintiffs claims are not barred by Section 230, it is the sum of Google's conduct that must be considered when assessing whether the assistance was substantial. The *Halberstam* court identified six factors relevant to assessing whether the substantial assistance component is satisfied: "(1) the nature of the act encouraged, (2) the amount of assistance given by

[12] It may be that what is considered by one person to be "substantial assistance" is considered by another merely *de minimis* or inconsequential. But even if that is so, it would be a better procedure to leave that decision to fairly selected jurors with proper jury instructions explaining the "substantial assistance" element. But to me it is clear that ISIS could not exist and renew itself without constant recruitment of foot soldiers to carry out its violent missions, often at the cost of their own lives, so I regret that I cannot persuade my colleagues here to adopt a more permissive standard for substantial assistance.

defendant, (3) defendant's presence or absence at the time of the tort, (4) defendant's relation to the principal, (5) defendant's state of mind, and (6) the period of defendant's assistance." *Linde*, 882 F.3d at 329 (citing *Halberstam*, 705 F.2d at 483–84).

Under the first factor, the *Halberstam* court emphasized that the nature of the principal's act "dictates what aid might matter, *i.e.*, be substantial." 705 F.2d at 484. The remaining factors must be viewed through this lens. ISIS's long-running and far-ranging terrorist campaign depends on the continued provision of money and recruits. Google provided both. As the majority acknowledges, financial support is "indisputably important" to operating a terrorism campaign, and any money provided to the organization may aid its goals. *See id.* at 488; *Fields*, 881 F.3d at 748. The majority also acknowledges, in the context of reversing the district court's dismissal of *Taamneh*, that YouTube videos encourage ISIS's terrorism campaign—an enterprise that is "heavily dependent on social media platforms to recruit members, to raise funds, and to disseminate propaganda." Google provided free exposure to a dangerous organization, thereby facilitating ISIS's ability to reach and rouse prospective recruits. The *Gonzalez* complaint alleges that ISIS through YouTube exaggerated its territorial expansion by disseminating videos with maps showing ISIS's claims that it controlled certain regions where other groups had pledged allegiance to ISIS. The fourth factor also weighs in favor of recognizing substantial assistance: defendant's "relation" to the principal—or the extent to which an entity "may possess greater powers of suggestion." YouTube's role in cultivating extremist behavior has been widely acknowledged and the platform reaches a virtually unlimited number of potential recruits due to the ubiquity of the Internet. The sixth factor, "duration of

the assistance provided," concerns the length of time an alleged aider and abettor has been involved with the tortfeasor. *See Halberstam*, 705 F.2d at 484 (emphasis omitted). Though the complaint in *Gonzalez* lacks specific evidence about the length of time Google provided assistance to ISIS, Plaintiffs allege the placement of ISIS recruiting videos going back at least four years before the Paris Attacks, in 2014. The complaint also alleged through news sources that advertisements were placed on ISIS's YouTube videos as early as March 2015, three years before the Paris Attacks. I would hold that years of hosting ISIS content and providing it with a percentage of revenue is sufficient duration. Though Plaintiffs do not allege that Google shared ISIS's terrorist goals, *Halberstam* also directs that under the fifth factor, defendant's "state of mind," the court can consider the duration factor because it "almost certainly affects the quality and extent" of the aid, the amount of aid provided, and "it may afford evidence of the defendant's state of mind." *Id.* Even considering state of mind on its own and viewing that factor in light of "the nature of the act encouraged," *see id.*, providing financial assistance and exposure to—to put it mildly—a dangerous group, is sufficient for state of mind to weigh against Google. As I see it, the conduct of Google, Twitter, and Facebook as related to the risks of terrorist attacks by ISIS, absent their more active review and policing of sites, is either recklessly indifferent or willfully blind, as they enjoy increased advertising revenue associated with eyeballs on videos or posts about ISIS attacks.

Taken as true and viewed in the light most favorable to Plaintiffs, I would hold that these allegations establish that Google's assistance was sufficiently "substantial" for purposes of § 2333(d)(2). These same considerations apply

in all three cases, so in each I would hold there was substantial assistance for purposes of § 2333(d)(2).

I add a brief comment about the *Clayborn v. Twitter* case. There the majority would uphold dismissal of the claims because of its view that Plaintiffs do not plausibly allege that ISIS "committed, planned, or authorized" the San Bernardino attack, as is required under 18 U.S.C. § 2333(d)(2). The majority relies on a Sixth Circuit decision, *Crosby v Twitter, Inc.*, 921 F.3d 617 (6th Cir. 2019), but its reasoning is not persuasive and does not bind or even guide our circuit, because there, the complaint produced "no allegations that ISIS was involved with the Pulse Night Club shooting." *Id.* at 626. However, the record here is distinctly and plainly to the contrary: The complaint expressly alleges that prior to or during the attack, one of the perpetrators—Tashfeen Malik—declared on her Facebook page the two shooters' allegiance and loyalty to an ISIS leader. Two days after the attack, ISIS issued a statement on a radio station claiming responsibility for the attack. The FBI confirmed that one of the shooters, a few years before the attack, had face-to-face meetings with five people known to have "links to terrorism." Further, Plaintiffs allege that FBI investigators found an explosive device placed at the crime scene that was likely intended to be detonated by the arrival of first responders. A Department of Justice report described this as "a frequent, well documented practice in international terrorism incidents." Importantly, FBI investigators explained that this "terrorist tactic ha[d] been outlined in Al Qaeda's *Inspire Magazine*, as well as in ISIS's *Dabiq Magazine*." Plaintiffs allege that these magazines are disseminated on Defendants' platforms. Together, these allegations permit the fair inference that the attack which was planned for at least one year was inspired by—and implicitly authorized by—ISIS.

In my view, even if Malik had been "self-radicalized" without direct communications or meetings with ISIS operatives, Plaintiffs plausibly allege that the self-radicalization process included exposure to the violent recruiting videos of ISIS, along with lectures from incendiary advocates of violence against non-believers. According to the complaint, in Senate Judiciary Committee testimony, then-FBI Director James Comey described the pair as having "consum[ed] poison on the internet" and been "radicalized to jihadism and to martyrdom via social media platforms available to them." Finally, even assuming the perpetrators had little advance connection with ISIS, well-established principles of agency law illustrate that authorization can occur not only by advance planning, but also by ratification. *See Restatement (Third) of Agency*, § 4.01(1) (1933) (defining ratification as "the affirmance of a prior act done by another, whereby the act is given effect as if done by an agent acting with actual authority").[13] Because the San Bernardino

[13] Contrary to the majority's contention, there is support for applying common law agency principles to secondary liability for acts of international terrorism. For one thing, "statutes are presumed not to disturb the common law, 'unless the language of a statute [is] clear and explicit for this purpose.'" *State Eng'r of Nev. v. S. Fork Band of Te-Moak Tribe of W. Shoshone Indians of Nev.*, 339 F.3d 804, 814 (9th Cir. 2003) (quoting *Norfolk Redevelopment & Hous. Auth. v. Chesapeake & Potomac Tel. Co. of Va.*, 464 U.S. 30, 35 (1983)). In my view, nothing in the statute precludes consideration of common law principles. Second, the Supreme Court has stated that apparent authority principles "ha[ve] long been the settled rule in the federal system." *Am. Soc'y of Mechanical Eng'rs, Inc. v. Hydrolevel Corp.*, 456 U.S. 556, 567 (1982). Section 2333(d)(2) assigns liability for injuries arising from acts of international terrorism, where that act was authorized by a terrorist organization. *See* 18 U.S.C. § 2333(d)(2). In my view, asking whether a terrorist organization authorized a particular terrorist act is properly viewed under

shooters pledged themselves to ISIS before or during the attack, and an act is ratifiable "if the actor acted or purported to act as an agent on the person's behalf," *id.* § 4.03, the attack can be considered authorized by ISIS.

For the foregoing reasons, the complaint in *Clayborn* makes allegations sufficient to state a claim for liability under the ATA.

V

In my view, the claims asserted in the three complaints on appeal should all be sustained and permitted to go forward in discovery based on the statutory law standards above discussed. But even if I am incorrect in my view of the governing statutory law, those claims should be able to go forward with complaint amendment based on a still extant specialized federal common law in aid of national security against terrorism. After the general common law regime of *Swift v. Tyson* was overruled by *Erie*, a sphere of specialized federal common law remains and could support Plaintiffs' claims here. *See e.g.*, 19 Charles Alan Wright & Arthur R. Miller, *Federal Practice & Procedure* § 4514 (3d ed. 2021). As the Wright & Miller treatise explains, "the federal common law that has developed since *Erie* differs from the federal general common law [rejected in] *Swift v. Tyson* because it falls within an area of federal or national competence." *Id.* (footnote omitted); *see also* 17A *Moore's Federal Practice*, Civil § 124.40 (2020). Many federal court precedents have applied these principles, which are particularly well-suited when claims involve an area of

---

the common-law agency framework as a question of whether the perpetrator was acting as an agent of the terrorist organization.

heightened federal interest, such as international terrorism, or when gaps exist in a federal regulatory scheme. *E.g.*, *Boyle v. United Techs. Corp.*, 487 U.S. 500, 507–08 (1988); *Textile Workers Union of Am. v. Lincoln Mills of Ala.*, 353 U.S. 448, 456–57 (1957); *King Jewelry, Inc. v. Fed. Express Corp.*, 316 F.3d 961, 964–65 (9th Cir. 2003).[14]

Also, our court should not ignore other potential areas of human conduct that can be negatively impacted by an unregulated social media regime, coupled with efforts by groups hostile to the idea of American democracy to use social media in order to divide or terrorize our public. Areas of particular concern include impacts of social media in realms such as election law, the laws governing public order and protest, and even insurrection.

We should not of course ignore the tremendous, indeed almost unquantifiable, benefits to the public from social media. Social media permits friends to stay in contact, as for example with a club or group from high school or college, lets people make new friends, or even lets people see or be exposed to new sights from different parts of the world. People met through social media, who may have different interests, perspectives, and priorities from other social media users, can in many cases enrich those users' lives. Places visited on the internet, often encouraged or directed through social media, can serve the same benign function. But at the

[14] Contrary to the majority's contention, my view on when federal common law may be created is narrow. Though the federal courts "are not free to manufacture entirely new causes of action merely because the political branches have not acted," I believe that we can act where gaps are present in an existing federal statutory scheme and the claim involved is one of unique federal concern.

same time, benefit alone cannot end the inquiry. Social media activities also carry with them some risks and detriments to the public. For example, there is no doubt that modern pharmaceutical drugs give benefits to the public that were impossible at earlier times and are greatly valued by those who use them. But drugs can also have harmful impacts and, accordingly, they are regulated by the Food & Drug Administration. Similarly, modern aircraft help people move from one part of our world to another with great speed and ease, but we regulate airlines through the Federal Aviation Administration. One could go on and on as almost every major activity in the modern world faces some type of federal regulation.

This regulation of the social media companies would best be examined by congressional committees with subpoena power and the ability to create new regulatory laws if needed and desirable. Or the government could create a new federal agency or Board or add powers or some supplemental standards to an existing federal agency, leaving the regulation of social media in part to a federal executive agency that is committed to bringing its technical expertise and knowledge of any areas of specialized federal concerns such as international terrorism and threats to democracy to bear on this issue. A specialized federal agency could call witnesses for testimony, assist meaningfully in a congressional task to prepare appropriate legislative guidance or prohibitions, have investigators to look into areas of concern, establish regulatory standards, and possibly also include an arm to enforce the law and its standards. *See, e.g.*, *Myers v. United States*, 272 U.S. 52, 129 (1926) (recognizing congressional authority to create federal agencies and define their scope and jurisdiction).

VI

These cases, and others like them pending in the federal courts, try for basic justice, but there is a fundamental question whether the federal courts are best suited to deliver it. I conclude with the following thoughts.

First, it would be preferable if the political branches of government, the legislature or the Executive Branch, would seriously grapple with the issue of unregulated social media power being used to amplify or to distort views asserted by users, and sometimes even by hostile nations using social media to wage asymmetric warfare or to impair democracy. But if Congress continues to sleep at the switch of social media regulation in the face of courts broadening what appears to have been its initial and literal language and expressed intention under Section 230, then it must fall to the federal courts to consider rectifying those errors itself by providing remedies to those who are injured by dangerous and unreasonable conduct.

Second, it would be preferable if the social media companies monitored their own activities sufficiently to protect the public, but in my view, to date they have not done that. It was one thing, at the dawn of the Internet era, to give protection to Internet companies to facilitate growth. But it is quite another thing to provide broad immunity at a time such as now when such companies are remarkably large and with massive staffs and perhaps the best technical abilities. It is not realistic to anticipate that social media companies will self-police adequately in the face of their incentives to maximize profits by maximizing advertising revenues, which means increasing the eyeballs directed to their websites. The large corporations controlling the platforms at issue in these

appeals can instead be expected to act in their own best financial interest, and to me, it makes absolutely no sense to leave such decisions to the self-interested proclamations of CEOs or other employees of the various social media companies.[15] Society for centuries has known that it is folly to ask the fox to guard the henhouse.

Third, the problem with a lack of social media regulation goes even beyond the dreadfully important subject of terrorism. Indeed, in connection with 21st-century political elections, some commenters have expressed concerns that social media has the ability to distort and tribalize public opinion, to spread falsehoods as well as truth, and to funnel like-minded news reports to groups in a way that makes them think there are "alternative facts" or "competing realities" that exist, rather than recognize more correctly that there are "truth" and "lies."[16]

Fourth, to the extent any of our Ninth Circuit precedent stands in the way of a sensible resolution of claims like those presented on appeal here, where terrorist organizations like ISIS have obviously played Google and YouTube like a fiddle, then in my view we should take these or other related cases *en banc* to give a full review.

---

[15] *E.g.*, 1 ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 13 (1776) ("It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest.").

[16] *See* Ross Douthat, *Why Do So Many Americans Think the Election Was Stolen?*, N.Y. TIMES (Dec. 5, 2020), https://www.nytimes.com/2020/12/05/opinion/sunday/trump-election-fraud.html?smid=tw-share.

Fifth, because the issues are difficult and only the Supreme Court can speak with authority ultimately on federal law, it would be desirable for the Supreme Court to take up the subject of Section 230 immunity and perhaps any related First Amendment issues, to the extent claims relating to terrorist speech are properly considered under that framework. Justice Oliver Wendell Holmes, Jr. made famous and enshrined in our law the idea that: "The life of the law has not been logic, it has been experience." OLIVER WENDELL HOLMES, JR., THE COMMON LAW, Lecture I (1881). But when almost all claims against social media companies are dismissed at the outset because of an overbroad view of Section 230 immunity, how is society to develop the experience that can guide its development of law in a sensible way that protects people from undue harm? Justice Holmes also developed the idea that speech should not be constrained absent "clear and present danger," *see Schenck v. United States*, 249 U.S. 47 (1919). To some degree this test still resounds in our First Amendment law. *See United States v. Alvarez*, 617 F.3d 1198, 1214 (9th Cir. 2010). A variation on this view culminated in *Brandenburg v. Ohio*, 395 U.S. 444 (1969), where the Supreme Court suggested that imminent lawless action was necessary before speech should be constrained. But perhaps given the current state of society, and the catastrophic dangers to the public that can be posed by terrorist activities, public safety may require that speech be limited when it poses a clear and increasing or gathering danger, rather than only "imminent" danger as reflected in *Brandenburg*, which I consider the Supreme Court's last word on this subject.

I also note that Oliver Wendell Holmes, Jr.'s famous pen pal and intellectual collaborator, Sir Frederick Pollock,[17] in his beginning primer of the law of torts, suggested that a principal force underlying all the varied types of tort cases was the desire of courts to provide a doctrinal basis for remedy in the case of injuries from harmful and unreasonable conduct. Pollock suggested that a "tort is an act or omission (not merely the breach of a duty arising out of a personal relation, or undertaken by contract) which is related to harm suffered by a determinate person in one of the following ways." *See* SIR FREDERICK POLLOCK, THE LAW OF TORTS: A TREATISE ON THE PRINCIPLES OF OBLIGATIONS ARISING FROM CIVIL WRONGS IN THE COMMON LAW 20 (4th ed. 1895). Among those ways a person can be harmed were these two, which are pertinent in assessing whether Plaintiffs' claims can be asserted as part of a federal common law: "(c) it may be an act or omission causing harm which the person so acting or so omitting did not intend to cause, but might and should with due diligence have foreseen and prevented," and "(d) it may in special cases consist in not avoiding or preventing that which the party was bound, absolutely or within limits to avoid or prevent." *Id.* Here, it could be expected that through federal common law development or statutory positive law, the social media companies will be held to some reasonable standard of conduct when they have

[17] *See* Oliver Wendell Holmes Jr. & Sir Frederick Pollock, Holmes–Pollock Letters: The Correspondence of Mr Justice Holmes and Sir Frederick Pollock, 1874–1932 (2d ed. 1961).

failed to regulate their own actions in the interests of the public.[18]

As a matter of federal common law, I would hold that when social media companies in their platforms use systems or procedures that are unreasonably dangerous to the public—as in the case where their systems line up repeated messages in aid of terrorists like ISIS—or when they omit to act to avoid harm when omitting the act is unreasonably dangerous to the public—as in the case where they fail to review and self-regulate their websites adequately to notice and remove propaganda videos from ISIS that are likely to cause harm—then there should be a federal common law claim available against them. Consider the most widely used standard for products liability cases. *See Restatement (Second) of Torts*, § 402A (1965). This suggests that manufacturers are responsible in tort if they make unreasonably dangerous products that cause individual or social harm. Section 402A states: "One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused" to the user or a third party. *Id.* Here and similarly, social media companies should be viewed as making and "selling" their social media products through the device of forced advertising under the eyes of users. Viewed in this light, they should be tested under a federal tort principle with a standard similar to and adapted from this *Restatement* language under a federal common law

[18] Developing federal common law on these issues will require the diligent and combined efforts of the federal courts and of legal scholars. *See, e.g.*, Hon. Wade H. McCree, Jr., *The Annual John Randolph Tucker Lecture, Partners in a Process: The Academy and the Courts*, 37 WASH. & LEE. L. REV. 1041 (1981).

development. If social media companies use "neutral" algorithms that cause unreasonably dangerous consequences, under proper standards of law with limiting jury instructions, they might be held responsible. Developing a federal common law standard would be superior to merely dismissing all claims against social media companies based on an over-broad interpretation of Section 230 delivering a blanket immunity, which in my view is inconsistent with congressional intent and detrimental to the interests of the general public.

ATTACHMENT A

KATZMANN, *Chief Judge*, concurring in part and dissenting in part:

I agree with much of the reasoning in the excellent majority opinion, and I join that opinion except for Parts I and II of the Discussion. But I must respectfully part company with the majority on its treatment of Facebook's friend- and content-suggestion algorithms under the Communications Decency Act ("CDA").[1]

---

[1] I agree with the majority that the CDA's exception for enforcement of criminal laws, 47 U.S.C. § 230(e)(1), does not apply to plaintiffs' claims, *see ante*, at 50-54. However, I find the question to be somewhat closer than the majority does, in part because some of the statutes enumerated in § 230(e)(1) *themselves* contain civil remedies. Section 230(e)(1) states that "[n]othing in [§ 230] shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute." One of those enumerated chapters—Chapter 110 of Title 18—includes a civil suit provision for victims of specific child sex crimes. *See* 18 U.S.C. § 2255. Meanwhile, 47 U.S.C. § 223—which prohibits obscene or harassing phone calls—specifies that civil fines may be levied "pursuant to civil action by," or "after appropriate administrative proceedings" of, the Federal Communications Commission ("FCC"), and it authorizes the Attorney General to bring civil suits to enjoin practices that violate the statute. 47 U.S.C. § 223(b)(5)(B)-(b)(6). If § 230(e)(1) covers "enforcement" of the listed chapters in their entirety, it is difficult to see how it would not cover other provisions that authorize civil suits for violations of criminal laws, particularly given that the enumerated list is followed by "or any *other* criminal law."

However, as detailed *post*, § 230 was designed as a private-sector-driven alternative to a Senate plan that would allow the FCC "either civilly or criminally, to punish people" who put objectionable material on the Internet. 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox); *accord id.* at 22,045-46 (statement of Rep. Wyden); *see Reno v. ACLU*, 521 U.S. 844, 859 & n.24 (1997). On the House floor, author Christopher Cox disparaged the idea of FCC enforcement and then stated: "Certainly, *criminal* enforcement of our obscenity laws as an adjunct is a useful way of punishing the truly

As to the reasons for my disagreement, consider a hypothetical. Suppose that you are a published author. One day, an acquaintance calls. "I've been reading over everything you've ever published," he informs you. "I've also been looking at everything you've ever said on the Internet. I've done the same for this other author. You two have very similar interests; I think you'd get along." The acquaintance then gives you the other author's contact information and photo, along with a link to all her published works. He calls back three more times over the next week with more names of writers you should get to know.

Now, you might say your acquaintance fancies himself a matchmaker. But would you say he's acting as the *publisher* of the other authors' work?

Facebook and the majority would have us answer this question "yes." I, however, cannot do so. For the scenario I have just described is little different from how Facebook's algorithms allegedly work. And while those algorithms do end up showing users profile, group, or event pages written by other users, it strains

---

guilty." 141 Cong. Rec. 22,045 (emphasis added). This history, along with the provision's title, strongly suggests that § 230(e)(1) was intended as a narrow criminal-law exception. It would be odd, then, to read § 230(e)(1) as allowing for civil enforcement by, among others, the FCC, even if only in aid of criminal law enforcement.

the English language to say that in targeting and recommending these writings to users—and thereby forging connections, developing new social networks—Facebook is acting as "the *publisher* of . . . information provided by another information content provider." 47 U.S.C. § 230(c)(1) (emphasis added).

It would be one thing if congressional intent compelled us to adopt the majority's reading. It does not. Instead, we today extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another. Neither the impetus for nor the text of § 230(c)(1) requires such a result. When a plaintiff brings a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals, the CDA does not and should not bar relief.

The Anti-Terrorism Act ("ATA") claims in this case fit this bill. According to plaintiffs' Proposed Second Amended Complaint ("PSAC")—which we must take as true at this early stage—Facebook has developed "sophisticated algorithm[s]" for bringing its users together. App'x 347 ¶ 622. After collecting mountains of data about each user's activity on and off its platform, Facebook

unleashes its algorithms to generate friend, group, and event suggestions based on what it perceives to be the user's interests. *Id.* at 345-46 ¶¶ 608-14. If a user posts about a Hamas attack or searches for information about a Hamas leader, Facebook may "suggest" that that user become friends with Hamas terrorists on Facebook or join Hamas-related Facebook groups. By "facilitat[ing] [Hamas's] ability to reach and engage an audience it could not otherwise reach as effectively," plaintiffs allege that Facebook's algorithms provide material support and personnel to terrorists. *Id.* at 347 ¶ 622; *see id.* at 352-58 ¶¶ 646-77. As applied to the algorithms, plaintiffs' claims do not seek to punish Facebook for the content others post, for deciding whether to publish third parties' content, or for editing (or failing to edit) others' content before publishing it. In short, they do not rely on treating Facebook as "the publisher" of others' information. Instead, they would hold Facebook liable for its affirmative role in bringing terrorists together.

When it comes to Facebook's algorithms, then, plaintiffs' causes of action do not run afoul of the CDA. Because the court below did not pass on the merits of the ATA claims pressed below, I would send this case back to the district court to decide the merits in the first instance. The majority, however, cuts off all possibility

for relief based on algorithms like Facebook's, even if these or future plaintiffs could prove a sufficient nexus between those algorithms and their injuries. In light of today's decision and other judicial interpretations of the statute that have generally immunized social media companies—and especially in light of the new reality that has evolved since the CDA's passage—Congress may wish to revisit the CDA to better calibrate the circumstances where such immunization is appropriate and inappropriate in light of congressional purposes.

I.

To see how far we have strayed from the path on which Congress set us out, we must consider where that path began. What is now 47 U.S.C. § 230 was added as an amendment to the Telecommunications Act of 1996, a statute designed to deregulate and encourage innovation in the telecommunications industry. Pub. L. 104-104, § 509, 110 Stat. 56, 56, 137-39; *see Reno*, 521 U.S. at 857. Congress devoted much committee attention to traditional telephone and broadcast media; by contrast, the Internet was an afterthought, addressed only through floor amendments or in conference. *Reno*, 521 U.S. at 857-58. Of the myriad issues the emerging Internet implicated, Congress tackled only one: the ease with which the

Internet delivers indecent or offensive material, especially to minors. *See* Telecommunications Act of 1996, tit. V, subtit. A, 110 Stat. at 133-39. And § 230 provided one of two alternative ways of handling this problem.

The action began in the Senate. Senator James J. Exon introduced the CDA on February 1, 1995. *See* 141 Cong. Rec. 3,203. He presented a revised bill on June 9, 1995, "[t]he heart and the soul" of which was "its protection for families and children." *Id.* at 15,503 (statement of Sen. Exon). The Exon Amendment sought to reduce the proliferation of pornography and other obscene material online by subjecting to civil and criminal penalties those who use interactive computer services to make, solicit, or transmit offensive material. *Id.* at 15,505.

The House of Representatives had the same goal—to protect children from inappropriate online material—but a very different sense of how to achieve it. Congressmen Christopher Cox (R-California) and Ron Wyden (D-Oregon) introduced an amendment to the Telecommunications Act, entitled "Online Family Empowerment," about two months after the revised CDA appeared in the Senate. *See id.* at 22,044. Making the argument for their amendment during the House floor debate, Congressman Cox stated:

> We want to make sure that everyone in America has an open invitation and feels welcome to participate in the Internet. But as you know, there is some reason for people to be wary because, as a Time Magazine cover story recently highlighted, there is in this vast world of computer information, a literal computer library, some offensive material, some things in the bookstore, if you will, that our children ought not to see.
>
> As the parent of two, I want to make sure that my children have access to this future and that I do not have to worry about what they might be running into on line. I would like to keep that out of my house and off my computer.

Id. at 22,044-45. Likewise, Congressman Wyden said: "We are all against smut and pornography, and, as the parents of two small computer-literate children, my wife and I have seen our kids find their way into these chat rooms that make their middle-aged parents cringe." *Id.* at 22,045.

As both sponsors noted, the debate between the House and the Senate was not over the CDA's primary purpose but rather over the best means to that shared end. *See id.* (statement of Rep. Cox) ("How should we do this? . . . Mr. Chairman, what we want are results. We want to make sure we do something that actually works."); *id.* (statement of Rep. Wyden) ("So let us all stipulate right at the outset the importance of protecting our kids and going to the issue of the best way to do it."). While the Exon Amendment would have the FCC regulate online obscene

materials, the sponsors of the House proposal "believe[d] that parents and families are better suited to guard the portals of cyberspace and protect our children than our Government bureaucrats." *Id.* at 22,045 (statement of Rep. Wyden). They also feared the effects the Senate's approach might have on the Internet itself. *See id.* (statement of Rep. Cox) ("[The amendment] will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the Internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the Internet . . . ."). The Cox-Wyden Amendment therefore sought to empower interactive computer service providers to self-regulate, and to provide tools for parents to regulate, children's access to inappropriate material. *See* S. Rep. No. 104-230, at 194 (1996) (Conf. Rep.); 141 Cong. Rec. 22,045 (statement of Rep. Cox).

There was only one problem with this approach, as the House sponsors saw it. A New York State trial court had recently ruled that the online service Prodigy, by deciding to remove certain indecent material from its site, had become a "publisher" and thus was liable for defamation when it failed to remove other objectionable content. *Stratton-Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710,

at *4 (N.Y. Sup. Ct. May 24, 1995) (unpublished). The authors of § 230 saw the *Stratton-Oakmont* decision as indicative of a "legal system [that] provides a massive disincentive for the people who might best help us control the Internet to do so." 141 Cong. Rec. 22,045 (statement of Rep. Cox). Cox-Wyden was designed, in large part, to remove that disincentive. *See* S. Rep. No. 104-230, at 194.

The House having passed the Cox-Wyden Amendment and the Senate the Exon Amendment, the conference committee had before it two alternative visions for countering the spread of indecent online material to minors. The committee chose not to choose. Congress instead adopted both amendments as part of a final Communications Decency Act. *See* Telecommunications Act of 1996, §§ 502, 509, 110 Stat. at 133-39; *Reno*, 521 U.S. at 858 n.24.[2] The Supreme Court promptly struck down two major provisions of the Exon Amendment as unconstitutionally

[2] It helped that the Cox-Wyden Amendment exempted from its deregulatory regime the very provisions that the Exon Amendment strengthened, *see* Telecommunications Act of 1996, §§ 502, 507-508, 509(d)(1), 110 Stat. at 133-39, and that Congress stripped from the House bill a provision that would have denied jurisdiction to the FCC to regulate the Internet, *compare id.* § 509, 110 Stat. at 138 (eliminating original § 509(d)), *with* 141 Cong. Rec. 22,044 (including original § 509(d)).

overbroad under the First Amendment, leaving the new § 230 as the dominant force for securing decency on the Internet. *See Reno*, 521 U.S. at 849.

Section 230 overruled *Stratton-Oakmont* through two interlocking provisions, both of which survived the legislative process unscathed. The first, which is at issue in this case, states 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." 47 U.S.C. § 230(c)(1). The second provision eliminates liability for interactive computer service providers and users for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be . . . objectionable," or "any action taken to enable or make available to . . . others the technical means to restrict access to [objectionable] material." *Id.* § 230(c)(2). These two subsections tackle, in overlapping fashion, the two jurisprudential moves of the *Stratton-Oakmont* court: first, that Prodigy's decision to screen posts for offensiveness rendered it "a publisher rather than a distributor," 1995 WL 323710, at *4; and second, that by making good-faith efforts to remove offensive material Prodigy became liable for any actionable material it did *not* remove.

The legislative history illustrates that in passing § 230 Congress was focused squarely on protecting minors from offensive online material, and that it sought to do so by "empowering parents to determine the content of communications their children receive through interactive computer services." S. Rep. No. 104-230, at 194. The "policy" section of § 230's text reflects this goal. *See* 47 U.S.C. § 230(b)(3)-(4).[3] It is not surprising, then, that Congress emphasized the narrow civil liability shield that became § 230(c)(2), rather than the broad rule of construction laid out in § 230(c)(1). Indeed, the conference committee summarized § 230 by stating that it "provides 'Good Samaritan' protections from civil liability for providers or users of an interactive computer service for actions to restrict or

[3] The policy section of the statute also expresses Congress's desire "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(2). It is therefore true that "Section 230 was enacted, *in part*, to maintain the robust nature of Internet communication." *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (emphasis added) (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997)); *see ante*, at 24. As the legislative history laid out in this opinion shows, however, one cannot fully understand the purpose of § 230 without considering that it was one chamber's proposal in a disagreement between the two houses of Congress over how best to shield children from indecent material, and that in that contest the House was principally concerned with two things: (1) overruling *Stratton-Oakmont* and (2) preventing "a Federal Computer Commission with an army of bureaucrats regulating the Internet." 141 Cong. Rec. 22,045 (statement of Rep. Cox).

to enable restriction of access to objectionable online material"—a description that could just as easily have applied to § 230(c)(2) alone. S. Rep. No. 104-230, at 194. Congress also titled the entirety of § 230(c) "Protection for 'Good Samaritan' blocking and screening of offensive material," suggesting that the definitional rule outlined in § 230(c)(1) may have been envisioned as supporting or working in tandem with the civil liability shield in § 230(c)(2).

None of this is to say that § 230(c)(1) exempts interactive computer service providers from publisher treatment only when they remove indecent content. Statutory text cannot be ignored, and Congress grabbed a bazooka to swat the *Stratton-Oakmont* fly. Whatever prototypical situation its drafters may have had in mind, § 230(c)(1) does not limit its protection to situations involving "obscene material" provided by others, instead using the expansive word "information."[4]

---

[4] This point—that Congress chose broader language than may have been necessary to accomplish its primary goal—should not be confused with the Seventh Circuit's rationale for § 230(c)(1)'s general application: that "a law's scope often differs from its genesis." *See Chi. Lawyers Cmte. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008). True as this axiom might be, it does not apply here—the language of § 230(c)(1) remained untouched from introduction to passage. Nor is there any evidence from the legislative record that interest groups altered the statutory language. *But cf. id.* ("Once the legislative process gets rolling, interest groups seek (and often obtain) other provisions."). That § 230(c)(1)'s breadth flowed from Congress's desire to

Illuminating Congress's original intent does, however, underscore the extent of § 230(c)(1)'s subsequent mission creep. Given how far both Facebook's suggestion algorithms and plaintiffs' terrorism claims swim from the shore of congressional purpose, caution is warranted before courts extend the CDA's reach any further.

II.

With the CDA's background in mind, I turn to the text. By its plain terms, § 230 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. *Contra ante*, at 30-31, 33-34, 49. It states, more specifically, 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." 47 U.S.C. § 230(c)(1) (emphases added). "Here grammar and usage establish that 'the' is a function word indicating that a following noun or noun equivalent is definite . . . ." *Nielsen v. Preap*, 139 S. Ct. 954, 965 (2019) (citation and internal quotation marks omitted).

---

overrule *Stratton-Oakmont*, rather than from mere interest group protectionism, matters.

The word "publisher" in this statute is thus inextricably linked to the "information provided by another." The question is whether a plaintiff's claim arises from a third party's information, and—crucially—whether to establish the claim the court must necessarily view the defendant, not as a publisher in the abstract, but rather as *the* publisher of that third-party information. *See FTC v. LeadClick Media, LLC*, 838 F.3d 158, 175 (2d Cir. 2016) (stating inquiry as "whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content provided by another").

For this reason, § 230(c)(1) does not necessarily immunize defendants from claims based on promoting content or selling advertising, even if those activities might be common among publishing companies nowadays. A publisher might write an email promoting a third-party event to its readers, for example, but the publisher would be the author of the underlying content and therefore not immune from suit based on that promotion. *See* 47 U.S.C. § 230(c)(1), (f)(3). Similarly, the fact that publishers may sell advertising based on user data does not immunize the publisher if someone brings a claim based on the publisher's selling of the data, because the claim would not treat the defendant as the publisher of a

third party's content. *Cf. Oberdorf v. Amazon.com Inc.*, No. 18-1041, 2019 WL 2849153, at *12 (3d Cir. July 3, 2019) (holding that the CDA does not bar claims against Amazon.com "to the extent that" they "rely on Amazon's role as an actor in the sales process," including both "selling" and "marketing"). Section 230(c)(1) limits liability based on the function the defendant performs, not its identity.

Accordingly, our precedent does not grant publishers CDA immunity for the full range of activities in which they might engage. Rather, it "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" provided by another for publication. *LeadClick*, 838 F.3d at 174 (citation and internal quotation marks omitted); *accord Oberdorf*, 2019 WL 2849153, at *10; *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016); *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 407 (6th Cir. 2014); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009); *Zeran*, 129 F.3d at 330; *see Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014); *Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc.*, 206 F.3d 980, 986 (10th Cir. 2000). For instance, a claim against a newspaper based on the content of a classified ad (or the decision to publish or

withdraw that ad) would fail under the CDA not because newspapers traditionally publish classified ads, but rather because such a claim would necessarily treat the newspaper as the publisher of the ad-maker's content. Similarly, the newspaper does not act as an "information content provider"—and thus maintains its CDA protection—when it decides to run a classified ad because it neither "creates" nor "develops" the information in the ad. 47 U.S.C. § 230(f)(3).

This case is different. Looking beyond Facebook's "broad statements of immunity" and relying "rather on a careful exegesis of the statutory language," *Barnes*, 570 F.3d at 1100, the CDA does not protect Facebook's friend- and content-suggestion algorithms. A combination of two factors, in my view, confirms that claims based on these algorithms do not inherently treat Facebook as the publisher of third-party content.[5] First, Facebook uses the algorithms to create and communicate its own message: that it thinks you, the reader—you, specifically—will like this content. And second, Facebook's suggestions contribute to the

[5] Many of Facebook's algorithms mentioned in the PSAC, such as its third-party advertising algorithm, its algorithm that places content in a user's newsfeed, and (based on the limited description in the PSAC) its video recommendation algorithm, remain immune under the analysis I set out here.

creation of real-world social networks. The result of at least some suggestions is not just that the user consumes a third party's content. Sometimes, Facebook's suggestions allegedly lead the user to become part of a unique global community, the creation and maintenance of which goes far beyond and differs in kind from traditional editorial functions.

It is true, as the majority notes, *see ante*, at 47, that Facebook's algorithms rely on and display users' content. However, this is not enough to trigger the protections of § 230(c)(1). The CDA does not mandate "a 'but-for' test that would provide immunity . . . solely because a cause of action would not otherwise have accrued but for the third-party content." *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019). Rather, to fall within § 230(c)(1)'s radius, the claim at issue must inherently fault the defendant's activity as the publisher of specific third-party content. Plaintiffs' claims about Facebook's suggestion algorithms do not do this. The complaint alleges that "Facebook collects detailed information about its users, including, inter alia, the content they post, type of content they view or engage with, people they communicate with, groups they belong to and how they interact with such groups, visits to third party websites,

apps and Facebook partners." App'x 345 ¶ 608. Then the algorithms "utilize the collected data to suggest friends, groups, products, services and local events, and target ads" based on each user's input. *Id.* at 346 ¶ 610.

If a third party got access to Facebook users' data, analyzed it using a proprietary algorithm, and sent its own messages to Facebook users suggesting that people become friends or attend one another's events, the third party would not be protected as "the publisher" of the users' information. Similarly, if Facebook were to use the algorithms to target *its own* material to particular users, such that the resulting posts consisted of "information provided by" Facebook rather than by "another information content provider," § 230(c)(1), Facebook clearly would not be immune for that independent message.

Yet that is ultimately what plaintiffs allege Facebook is doing. The PSAC alleges that Facebook "actively provides 'friend suggestions' between users who have expressed similar interests," and that it "actively suggests groups and events to users." App'x 346 ¶¶ 612-13. Facebook's algorithms thus allegedly provide the user with a message from Facebook. Facebook is telling users—perhaps implicitly, but clearly—that they would like these people, groups, or events. In this respect,

Facebook "does not merely provide a framework that could be utilized for proper or improper purposes; rather, [Facebook's] work in developing" the algorithm and suggesting connections to users based on their prior activity on Facebook, including their shared interest in terrorism, "is directly related to the alleged illegality of the site." *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1171 (9th Cir. 2008) (en banc). The fact that Facebook also publishes third-party content should not cause us to conflate its two separate roles with respect to its users and their information. Facebook may be immune under the CDA from plaintiffs' challenge to its allowance of Hamas accounts, since Facebook acts solely as the publisher of the Hamas users' content. That does not mean, though, that it is also immune when it conducts statistical analyses of that information and delivers a message based on those analyses.

Moreover, in part through its use of friend, group, and event suggestions, Facebook is doing more than just publishing content: it is proactively creating networks of people. Its algorithms forge real-world (if digital) connections through friend and group suggestions, and they attempt to create similar connections in the physical world through event suggestions. The cumulative effect of

recommending several friends, or several groups or events, has an impact greater than the sum of each suggestion. It envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own. According to the allegations in the complaint, Facebook designed its website for this very purpose. "Facebook has described itself as a provider of products and services that enable users . . . to find and connect with other users . . . ." App'x 250 ¶ 129. CEO Mark Zuckerberg has similarly described Facebook as "build[ing] tools to help people connect with the people they want," thereby "extending people's capacity to build and maintain relationships." *Id.* at 251 ¶ 132. Of course, Facebook is not the only company that tries to bring people together this way, and perhaps other publishers try to introduce their readers to one another. Yet the creation of social networks goes far beyond the traditional editorial functions that the CDA immunizes.

Another way to consider the CDA immunity question is to "look . . . to what the duty at issue actually requires: specifically, whether the duty would necessarily require an internet company to monitor[, alter, or remove] third-party content." *HomeAway.com*, 918 F.3d at 682. Here, too, the claims regarding the

algorithms are a poor fit for statutory immunity. The duty not to provide material support to terrorism, as applied to Facebook's use of the algorithms, simply requires that Facebook not actively use that material to determine which of its users to connect to each other. It could stop using the algorithms altogether, for instance. Or, short of that, Facebook could modify its algorithms to stop them introducing terrorists to one another. None of this would change any underlying content, nor would it necessarily require courts to assess further the difficult question of whether there is an affirmative obligation to monitor that content.

In reaching this conclusion, I note that ATA torts are atypical. Most of the common torts that might be pleaded in relation to Facebook's algorithms "derive liability from behavior that is identical to publishing or speaking"—for instance, "publishing defamatory material; publishing material that inflicts emotional distress; or . . . attempting to de-publish hurtful material but doing it badly." *Barnes*, 570 F.3d at 1107. The fact that Facebook has figured out how to target material to people more likely to read it does not matter to a defamation claim, for instance, because the mere act of publishing in the first place creates liability.

The ATA works differently. Plaintiffs' material support and aiding and abetting claims premise liability, not on publishing *qua* publishing, but rather on Facebook's provision of services and personnel to Hamas. It happens that the way in which Facebook provides these benefits includes republishing content, but Facebook's duties under the ATA arise separately from the republication of content. *Cf. id.* (determining that liability on a promissory estoppel theory for promising to remove content "would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication"). For instance, the operation of the algorithms is allegedly provision of "expert advice or assistance," and the message implied by Facebook's prodding is allegedly a "service" or an attempt to provide "personnel." 18 U.S.C. § 2339A(b).

For these reasons, § 230(c)(1) does not bar plaintiffs' claims.

III.

Even if we sent this case back to the district court, as I believe to be the right course, these plaintiffs might have proven unable to allege that Facebook's matchmaking algorithms played a role in the attacks that harmed them. However,

assuming *arguendo* that such might have been the situation here, I do not think we should foreclose the possibility of relief in future cases if victims can plausibly allege that a website knowingly brought terrorists together and that an attack occurred as a direct result of the site's actions. Though the majority shuts the door on such claims, today's decision also illustrates the extensive immunity that the current formulation of the CDA already extends to social media companies for activities that were undreamt of in 1996. It therefore may be time for Congress to reconsider the scope of § 230.

As is so often the case with new technologies, the very qualities that drive social media's success—its ease of use, open access, and ability to connect the world—have also spawned its demons. Plaintiffs' complaint illustrates how pervasive and blatant a presence Hamas and its leaders have maintained on Facebook. Hamas is far from alone—Hezbollah, Boko Haram, the Revolutionary Armed Forces of Colombia, and many other designated terrorist organizations use Facebook to recruit and rouse supporters. Vernon Silver & Sarah Frier, *Terrorists Are Still Recruiting on Facebook, Despite Zuckerberg's Reassurances*, Bloomberg Businessweek (May 10, 2018), http://www.bloomberg.com/news/articles/2018-05-

10/terrorists-creep-onto-facebook-as-fast-as-it-can-shut-them-down. Recent news reports suggest that many social media sites have been slow to remove the plethora of terrorist and extremist accounts populating their platforms,[6] and that such efforts, when they occur, are often underinclusive. Twitter, for instance, banned the Ku Klux Klan in 2018 but allowed David Duke to maintain his account, *see* Roose & Conger, *supra*, while researchers found that Facebook removed fewer than half the terrorist accounts and posts those researchers identified, *see* Waters & Postings, *supra*, at 8; Desmond Butler & Barbara Ortulay, *Facebook Auto-Generates Videos Celebrating Extremist Images*, Assoc. Press (May 9, 2019), http://apnews.com/f97c24dab4f34bd0b48b36f2988952a4. Those whose accounts *are* removed often pop up again under different names or with slightly different

[6] *See, e.g.*, Gregory Waters & Robert Postings, *Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook* 8, Counter Extremism Project (May 2018), http://www.counterextremism.com/sites/default/files/Spiders%20of%20the%20Caliphate%20%28May%202018%29.pdf; Yaacov Benmeleh & Felice Maranz, *Israel Warns Twitter of Legal Action Over Requests to Remove Content*, Bloomberg (Mar. 20, 2018), http://www.bloomberg.com/news/articles/2018-03-20/israel-warns-twitter-of-legal-steps-over-incitement-to-terrorism; Mike Isaac, *Twitter Steps Up Efforts to Thwart Terrorists' Tweets*, N.Y. Times (Feb. 5, 2016), http://www.nytimes.com/2016/02/06/technology/twitter-account-suspensions-terrorism.html; Kevin Roose & Kate Conger, *YouTube to Remove Thousands of Videos Pushing Extreme Views*, N.Y. Times (June 5, 2019), http://www.nytimes.com/2019/06/05/business/youtube-remove-extremist-videos.html.

language in their profiles, playing a perverse and deadly game of Whack-a-Mole with Silicon Valley. *See* Isaac, *supra*; Silver & Frier, *supra*.

Of course, the failure to remove terrorist content, while an important policy concern, is immunized under § 230 as currently written. Until today, the same could not have been said for social media's unsolicited, algorithmic spreading of terrorism. Shielding internet companies that bring terrorists together using algorithms could leave dangerous activity unchecked.

Take Facebook. As plaintiffs allege, its friend-suggestion algorithm appears to connect terrorist sympathizers with pinpoint precision. For instance, while two researchers were studying Islamic State ("IS") activity on Facebook, one "received dozens of pro-IS accounts as recommended friends after friending just one pro-IS account." Waters & Postings, *supra*, at 78. More disturbingly, the other "received an influx of Philippines-based IS supporters and fighters as recommended friends after liking several non-extremist news pages about Marawi and the Philippines during IS's capture of the city." *Id.* News reports indicate that the friend-suggestion feature has introduced thousands of IS sympathizers to one another. *See* Martin Evans, *Facebook Accused of Introducing Extremists to One Another Through*

'Suggested Friends' Feature, The Telegraph (May 5, 2018), http://www.telegraph.co.uk/news/2018/05/05/facebook-accused-introducing-extremists-one-another-suggested.

And this is far from the only Facebook algorithm that may steer people toward terrorism. Another turns users' declared interests into audience categories to enable microtargeted advertising. In 2017, acting on a tip, ProPublica sought to direct an ad at the algorithmically-created category "Jew hater"—which turned out to be real, as were "German Schutzstaffel," "Nazi Party," and "Hitler did nothing wrong." Julia Angwin et al., *Facebook Enabled Advertises to Reach 'Jew Haters,'* ProPublica (Sept. 14, 2017), https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters. As the "Jew hater" category was too small for Facebook to run an ad campaign, "Facebook's automated system suggested 'Second Amendment' as an additional category . . . presumably because its system had correlated gun enthusiasts with anti-Semites." *Id.*

That's not all. Another Facebook algorithm auto-generates business pages by scraping employment information from users' profiles; other users can then "like" these pages, follow their posts, and see who else has liked them. Butler &

Ortutay, *supra*. ProPublica reports that extremist organizations including al-Qaida, al-Shabab, and IS have such auto-created pages, allowing them to recruit the pages' followers. *Id.* The page for al-Qaida in the Arabian Peninsula included the group's Wikipedia entry and a propaganda photo of the damaged USS Cole, which the group had bombed in 2000. *Id.* Meanwhile, a fourth algorithm integrates users' photos and other media to generate videos commemorating their previous year. *Id.* Militants get a ready-made propaganda clip, complete with a thank-you message from Facebook. *Id.*

This case, and our CDA analysis, has centered on the use of algorithms to foment terrorism. Yet the consequences of a CDA-driven, hands-off approach to social media extend much further. Social media can be used by foreign governments to interfere in American elections. For example, Justice Department prosecutors recently concluded that Russian intelligence agents created false Facebook groups and accounts in the years leading up to the 2016 election campaign, bootstrapping Facebook's algorithm to spew propaganda that reached between 29 million and 126 million Americans. *See* 1 Robert S. Mueller III, Special Counsel, *Report on the Investigation Into Russian Interference in the 2016 Presidential*

Election 24-26, U.S. Dep't of Justice (March 2019), http://www.justice.gov/storage/report.pdf. Russia also purchased over 3,500 advertisements on Facebook to publicize their fake Facebook groups, several of which grew to have hundreds of thousands of followers. *Id.* at 25-26. On Twitter, Russia developed false accounts that impersonated American people or groups and issued content designed to influence the election; it then created thousands of automated "bot" accounts to amplify the sham Americans' messages. *Id.* at 26-28. One fake account received over six million retweets, the vast majority of which appear to have come from real Twitter users. *See* Gillian Cleary, *Twitterbots: Anatomy of a Propaganda Campaign*, Symantec (June 5, 2019), http://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation. Russian intelligence also harnessed the reach that social media gave its false identities to organize "dozens of U.S. rallies," some of which "drew hundreds" of real-world Americans. Mueller, *Report*, *supra*, at 29. Russia could do all this only because social media is designed to target messages like Russia's to the users most susceptible to them.

While Russia's interference in the 2016 election is the best-documented example of foreign meddling through social media, it is not the only one. Federal

intelligence agencies expressed concern in the weeks before the 2018 midterm election "about ongoing campaigns by Russia, China and other foreign actors, including Iran," to "influence public sentiment" through means "including using social media to amplify divisive issues." Press Release, Office of Dir. of Nat'l Intelligence, Joint Statement from the ODNI, DOJ, FBI, and DHS: Combatting Foreign Influence in U.S. Elections, (Oct. 19, 2018), https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections. News reports also suggest that China targets state-sponsored propaganda to Americans on Facebook and purchases Facebook ads to amplify its communications. *See* Paul Mozur, *China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home*, N.Y. Times (Nov. 8, 2017), https://www.nytimes.com/2017/11/08/technology/china-facebook.html.

Widening the aperture further, malefactors at home and abroad can manipulate social media to promote extremism. "Behind every Facebook ad, Twitter feed, and YouTube recommendation is an algorithm that's designed to keep users using: It tracks preferences through clicks and hovers, then spits out a steady stream of content that's in line with your tastes." Katherine J. Wu, *Radical*

Ideas Spread Through Social Media. Are the Algorithms to Blame?, PBS (Mar. 28, 2019), https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms.

All too often, however, the code itself turns those tastes sour. For example, one study suggests that manipulation of Facebook's news feed influences the mood of its users: place more positive posts on the feed and users get happier; focus on negative information instead and users get angrier. Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788, 8789 (2014). This can become a problem, as Facebook's algorithm "tends to promote the most provocative content" on the site. Max Fisher, *Inside Facebook's Secret Rulebook for Global Political Speech*, N.Y. Times (Dec. 27, 2018), http://www.nytimes.com/2018/12/27/world/facebook-moderators.html. Indeed, "[t]he Facebook News Feed environment brings together, in one place, many of the influences that have been shown to drive psychological aspects of polarization." Jaime E. Settle, *Frenemies: How Social Media Polarizes America* (2018). Likewise, YouTube's video recommendation algorithm—which leads to more than 70 percent of time people spend on the platform—has been criticized for shunting visitors toward ever more extreme and divisive videos. Roose & Conger,

supra; *see* Jack Nicas, *How YouTube Drives People to the Internet's Darkest Corners*, Wall St. J. (Feb. 7, 2018), https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478. YouTube has fine-tuned its algorithm to recommend videos that recalibrate users' existing areas of interest and steadily steer them toward new ones—a modus operandi that has reportedly proven a real boon for far-right extremist content. *See* Kevin Roose, *The Making of a YouTube Radical*, N.Y. Times (June 8, 2019), http://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html.

There is also growing attention to whether social media has played a significant role in increasing nationwide political polarization. *See* Andrew Soergel, *Is Social Media to Blame for Political Polarization in America?*, U.S. News & World Rep. (Mar. 20, 2017), https://www.usnews.com/news/articles/2017-03-20/is-social-media-to-blame-for-political-polarization-in-america. The concern is that "web surfers are being nudged in the direction of political or unscientific propaganda, abusive content, and conspiracy theories." Wu, *Radical Ideas*, *supra*. By surfacing ideas that were previously deemed too radical to take seriously, social media mainstreams them, which studies show makes people "much more

open" to those concepts. Max Fisher & Amanda Taub, *How Everyday Social Media Users Become Real-World Extremists*, N.Y. Times (Apr. 25, 2018), http://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html. At its worst, there is evidence that social media may even be used to push people toward violence.[7] The sites are not entirely to blame, of course—they would not have such success without humans willing to generate and to view extreme content. Providers are also tweaking the algorithms to reduce their pull toward hate speech and other inflammatory material. *See* Isaac, *supra*; Roose & Conger, *supra*. Yet the dangers of social media, in its current form, are palpable.

While the majority and I disagree about whether § 230 immunizes interactive computer services from liability for all these activities or only some, it

---

[7] *See, e.g.*, Sarah Marsh, *Social Media Related to Violence by Young People, Say Experts*, The Guardian (Apr. 2, 2018), https://www.theguardian.com/media/2018/apr/02/social-media-violence-young-people-gangs-say-experts; Kevin Roose, *A Mass Murder of, and for, the Internet*, N.Y. Times (Mar. 15, 2019), https://www.nytimes.com/2019/03/15/technology/facebook-youtube-christchurch-shooting.html; Craig Timberg et al., *The New Zealand Shooting Shows How TouTube and Facebook Spread Hate and Violent Images—Yet Again*, Wash. Post (Mar. 15, 2019), https://www.washingtonpost.com/technology/2019/03/15/facebook-youtube-twitter-amplified-video-christchurch-mosque-shooting; Julie Turkewitz & Kevin Roose, *Who Is Robert Bowers, the Suspect in the Pittsburgh Synagogue Shooting?*, N.Y. Times (Oct. 27, 2018), https://www.nytimes.com/2018/10/27/us/robert-bowers-pittsburgh-synagogue-shooter.html.

is pellucid that Congress did not have any of them in mind when it enacted the CDA. The text and legislative history of the statute shout to the rafters Congress's focus on reducing children's access to adult material. Congress could not have anticipated the pernicious spread of hate and violence that the rise of social media likely has since fomented. Nor could Congress have divined the role that social media providers themselves would play in this tale. Mounting evidence suggests that providers designed their algorithms to drive users toward content and people the users agreed with—and that they have done it too well, nudging susceptible souls ever further down dark paths. By contrast, when the CDA became law, the closest extant ancestor to Facebook (and it was still several branches lower on the evolutionary tree) was the chatroom or message forum, which acted as a digital bulletin board and did nothing proactive to forge off-site connections.[8]

---

[8] *See* Caitlin Dewey, *A Complete History of the Rise and Fall—and Reincarnation!—of the Beloved '90s Chatroom*, Wash. Post (Oct. 30, 2014), http://www.washingtonpost.com/news/the-intersect/wp/2014/10/30/a-complete-history-of-the-rise-and-fall-and-reincarnation-of-the-beloved-90s-chatroom; *see also Then and Now: A History of Social Networking Sites*, CBS News, http://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites (last accessed July 9, 2019) (detailing the evolution of social media sites from Classmates, launched only "as a list of school affiliations" in December 1995; to "the very first social networking site" Six Degrees, which launched in May 1997 but whose networks were limited "due to the lack of people connected to the Internet";

Whether, and to what extent, Congress should allow liability for tech companies that encourage terrorism, propaganda, and extremism is a question for legislators, not judges. Over the past two decades "the Internet has outgrown its swaddling clothes," *Roommates.Com*, 521 F.3d at 1175 n.39, and it is fair to ask whether the rules that governed its infancy should still oversee its adulthood. It is undeniable that the Internet and social media have had many positive effects worth preserving and promoting, such as facilitating open communication, dialogue, and education. At the same time, as outlined above, social media can be manipulated by evildoers who pose real threats to our democratic society. A healthy debate has begun both in the legal academy[9] and in the policy

---

to Friendster, launched in March 2002 and "credited as giving birth to the modern social media movement"; to Facebook, which was "rolled out to the public in September 2006").

[9] *See, e.g.*, Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 Geo. L. Tech. Rev. 453, 454-55 (2018); Jeff Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 J. Tech. L. & Pol'y 123, 124 (2010); Daniela C. Manzi, *Managing the Misinformation Marketplace: The First Amendment and the Fight Against Fake News*, 87 Fordham L. Rev. 2623, 2642-43 (2019). Much of the enterprising legal scholarship debating the intersection of social media, terrorism, and the CDA comes from student Notes. *See, e.g.*, Jaime E. Freilich, Note, *Section 230's Liability Shield in the Age of Online Terrorist Recruitment*, 83 Brook. L. Rev. 675, 690-91 (2018); Anna Elisabeth Jayne Goodman, Note and Comment, *When You Give a Terrorist a Twitter: Holding Social Media Companies Liable for their Support of Terrorism*, 46 Pepp. L. Rev. 147, 182-86 (2018); Nicole Phe, Note, *Social Media Terror: Reevaluating Intermediary Liability*

community[10] about changing the scope of § 230. Perhaps Congress will clarify what I believe the text of the provision already states: that the creation of social networks reaches beyond the publishing functions that § 230 protects. Perhaps Congress will engage in a broader rethinking of the scope of CDA immunity. Or perhaps Congress will decide that the current regime best balances the interests involved. In the meantime, however, I cannot join my colleagues' decision to immunize Facebook's friend- and content-suggestion algorithms from judicial scrutiny. I therefore must in part respectfully dissent, as I concur in part.

Under the Communications Decency Act, 51 Suffolk U. L. Rev. 99, 126-30 (2018).

[10] *See, e.g.*, Tarleton Gillespie, *How Social Netowrks Set the Limits of What We Can Say Online*, Wired (June 26, 2018), http://www.wired.com/story/how-social-networks-set-the-limits-of-what-we-can-say-online; Christiano Lima, *How a Widening Political Rift Over Online Liability Is Splitting Washington*, Politico (July 9, 2019), http://www.politico.com/story/2019/07/09/online-industry-immunity-section-230-1552241; Mark Sullivan, *The 1996 Law That Made the Web Is in the Crosshairs*, Fast Co. (Nov. 29, 2018), http://www.fastcompany.com/90273352/maybe-its-time-to-take-away-the-outdated-loophole-that-big-tech-exploits; *cf.* Darrell M. West & John R. Allen, *How Artificial Intelligence Is Transforming the World*, Brookings (Apr. 24, 2018), http://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world ("The malevolent use of AI exposes individuals and organizations to unnecessary risks and undermines the virtues of the emerging technology.").