In the
United States Court of Appeals
For the Second Circuit

August Term, 2018
No. 18-397

STUART FORCE, individually and as Administrator on behalf of the Estate of TAYLOR FORCE, ROBBI FORCE, KRISTIN ANN FORCE, ABRAHAM RON FRAENKEL, individually and as Administrator on behalf of the Estate of YAAKOV NAFTALI FRAENKEL, and as the natural and legal guardian of minor plaintiffs A.H.H.F., A.L.F., N.E.F, N.S.F., and S.R.F., A.H.H.F., A.L.F., N.E.F., N.S.F., S.R.F., RACHEL DEVORA SPRECHER FRAENKEL, individually and as Administrator on behalf of the Estate of YAAKOV NAFTALI FRAENKEL and as the natural and legal guardian of minor plaintiffs A.H.H.F., A.L.F., N.E.F, N.S.F., and S.R.F., TZVI AMITAY FRAENKEL, SHMUEL ELIMELECH BRAUN, individually and as Administrator on behalf of the Estate of CHAYA ZISSEL BRAUN, CHANA BRAUN, individually and as Administrator on behalf of the Estate of CHAYA ZISSEL BRAUN, SHIMSHON SAM HALPERIN, SARA HALPERIN, MURRAY BRAUN, ESTHER BRAUN, MICAH LAKIN AVNI, individually and as Joint Administrator on behalf of the Estate of RICHARD LAKIN, MAYA LAKIN, individually and as Joint Administrator on behalf of the Estate of RICHARD LAKIN, MENACHEM MENDEL RIVKIN, individually and as the natural and legal guardian of minor plaintiffs S.S.R., M.M.R., R.M.R., S.Z.R., BRACHA RIVKIN, individually and as the natural and legal guardian of minor plaintiffs S.S.R., M.M.R., R.M.R., and S.Z.R., S.S.R., M.M.R., R.M.R., S.Z.R.,

Plaintiffs-Appellants,

v.

FACEBOOK, INC.,
Defendant-Appellee.[1]

Appeal from the United States District Court
for the Eastern District of New York.
No. 16-cv-5158 — Nicholas G. Garaufis, *Judge*.

ARGUED: FEBRUARY 25, 2019
DECIDED: JULY 31, 2019

Before: KATZMANN, *Chief Judge*, DRONEY, and SULLIVAN, *Circuit Judges*.

Plaintiffs-Appellants, U.S. citizen victims of Hamas terrorist attacks in Israel (or their representatives), appeal from a final judgment of the United States District Court for the Eastern District of New York (Garaufis, *J.*). Plaintiffs brought federal civil anti-terrorism and Israeli law claims against Defendant-Appellee Facebook, Inc., alleging that Facebook unlawfully assisted Hamas in those attacks. The district court dismissed the claims on the basis of 47 U.S.C. § 230(c)(1), which bars civil liability for claims that "treat[]" a "provider or user of an interactive computer service . . . as the publisher or speaker of any information provided by another

[1] The Clerk of the Court is directed to amend the official caption to conform to the above.

information content provider." We agree with the district court that Section 230(c)(1) bars plaintiffs' federal claims. We also conclude, upon a review of plaintiffs' assertion of diversity jurisdiction over their foreign law claims, 28 U.S.C. § 1332(a), that such jurisdiction is lacking, and we decline to exercise supplemental jurisdiction *sua sponte*. Accordingly, we **AFFIRM** the judgment of the district court as to plaintiffs' federal claims and **DISMISS** plaintiffs' foreign law claims.

Chief Judge KATZMANN concurs in this opinion except as to Parts I and II of the Discussion, concurs in the judgment with respect to plaintiffs' foreign law claims, and dissents from the judgment with respect to plaintiffs' federal claims.

MEIR KATZ (Robert J. Tolchin, *on the brief*), The Berkman Law Office, LLC, Brooklyn, New York, *for Plaintiffs-Appellants.*

CRAIG S. PRIMIS (K. Winn Allen, Matthew S. Brooker, *on the brief*), Kirkland & Ellis, LLP, Washington, DC, *for Defendant-Appellee.*

Sophia Cope, David Greene, Electronic Frontier Foundation, San Francisco, CA, *amicus curiae*.

DRONEY, *Circuit Judge*:

The principal question presented in this appeal is whether 47 U.S.C. § 230(c)(1), a provision enacted by the Communications Decency Act of 1996, shields Defendant-Appellee Facebook, Inc., from civil liability as to Plaintiffs-Appellants' federal anti-terrorism claims. Plaintiffs include the U.S. citizen victims, and relatives and representatives of the estates of those victims, of certain terrorist attacks committed by Hamas in Israel. They contend that Facebook unlawfully provided Hamas, a U.S.-designated foreign terrorist organization, with a communications platform that enabled those attacks.

The district court granted Facebook's motion to dismiss plaintiffs' First Amended Complaint under Federal Rule of Civil Procedure 12(b)(6) on the basis of Section 230(c)(1) immunity, an affirmative defense. After entering judgment without prejudice to moving to file an amended complaint, the district court denied with

prejudice plaintiffs' motion to file a second amended complaint on the basis that the proposed complaint did not cure the deficiencies in the First Amended Complaint.

On appeal, plaintiffs argue that the district court improperly dismissed their claims because Section 230(c)(1) does not provide immunity to Facebook under the circumstances of their allegations.

We conclude that the district court properly applied Section 230(c)(1) to plaintiffs' federal claims. Also, upon our review of plaintiffs' assertion of diversity jurisdiction over their foreign law claims, 28 U.S.C. § 1332(a), we conclude that such jurisdiction is lacking. Accordingly, we affirm the judgment of the district court as to the federal claims. We also dismiss the foreign law claims, but without prejudice.

FACTUAL AND PROCEDURAL BACKGROUND

I. Allegations in Plaintiffs' Complaint[2]

Because this case comes to us on a motion to dismiss, we recount the facts as plaintiffs provide them to us, treating as true the allegations in their complaint. *See Galper v. JP Morgan Chase Bank, N.A.*, 802 F.3d 437, 442 (2d Cir. 2015).

A. The Attacks

Hamas is a Palestinian Islamist organization centered in Gaza. It has been designated a foreign terrorist organization by the United States and Israel. Since it was formed in 1987, Hamas has conducted thousands of terrorist attacks against civilians in Israel.

Plaintiffs' complaint describes terrorist attacks by Hamas against five Americans in Israel between 2014 and 2016. Yaakov Naftali Fraenkel, a teenager, was kidnapped by a Hamas operative in

[2] As used here, the term "complaint" refers to both the allegations of the First Amended Complaint and those of the proposed second amended complaint, which sought to supplement the prior complaint.

2014 while walking home from school in Gush Etzion, near Jerusalem, and then was shot to death. Chaya Zissel Braun, a 3-month-old baby, was killed at a train station in Jerusalem in 2014 when a Hamas operative drove a car into a crowd. Richard Lakin died after Hamas members shot and stabbed him in an attack on a bus in Jerusalem in 2015. Graduate student Taylor Force was stabbed to death by a Hamas attacker while walking on the Jaffa boardwalk in Tel Aviv in 2016. Menachem Mendel Rivkin was stabbed in the neck in 2016 by a Hamas operative while walking to a restaurant in a town near Jerusalem. He suffered serious injuries but survived. Except for Rivkin, plaintiffs are the representatives of the estates of those who died in these attacks and family members of the victims.

B. Facebook's Alleged Role in the Attacks

1. How Facebook Works

Facebook operates an "online social network platform and communications service[]." App'x 230. Facebook users populate

their own "Facebook 'pages'" with "content," including personal identifying information and indications of their particular "interests." App'x 250–51, 345. Organizations and other entities may also have Facebook pages. Users can post content on others' Facebook pages, reshare each other's content, and send messages to one another. The content can be text-based messages and statements, photos, web links, or other information.

Facebook users must first register for a Facebook account, providing their names, telephone numbers, and email addresses. When registering, users do not specify the nature of the content they intend to publish on the platform, nor does Facebook screen new users based on its expectation of what content they will share with other Facebook users. There is no charge to prospective users for joining Facebook.[3]

[3] According to Facebook, hundreds of millions of Facebook pages are maintained on its platform.

Facebook does not preview or edit the content that its users post. Facebook's terms of service specify that a user "own[s] all of the content and information [the user] post[s] on Facebook, and [the user] can control how it is shared through [the user's] privacy and application settings." App'x 252 (alterations in original).

While Facebook users may view each other's shared content simply by visiting other Facebook pages and profiles, Facebook also provides a personalized "newsfeed" page for each user. Facebook uses algorithms—"a precisely defined set of mathematical or logical operations for the performance of a particular task," *Algorithm*, Oxford English Dictionary (3d ed. 2012)—to determine the content to display to users on the newsfeed webpage. Newsfeed content is displayed within banners or modules and changes frequently. The newsfeed algorithms—developed by programmers employed by Facebook—automatically analyze Facebook users' prior behavior on the Facebook website to predict and display the content that is most

likely to interest and engage those particular users. Other algorithms similarly use Facebook users' behavioral and demographic data to show those users third-party groups, products, services, and local events likely to be of interest to them.

Facebook's algorithms also provide "friend suggestions," which, if accepted by the user, result in those users seeing each other's shared content. App'x 346–47. The friend-suggestion algorithms are based on such factors as the users' common membership in Facebook's online "groups," geographic location, attendance at events, spoken language, and mutual friend connections on Facebook. App'x 346.

Facebook's advertising algorithms and "remarketing" technology also allow advertisers on Facebook to target specific ads to its users who are likely to be most interested in them and thus to be most beneficial to those advertisers. App'x 347. Those advertisements are displayed on the users' pages and other Facebook

webpages. A substantial portion of Facebook's revenues is from such advertisers.

2. Hamas's Use of Facebook[4]

Plaintiffs allege that Hamas used Facebook to post content that encouraged terrorist attacks in Israel during the time period of the attacks in this case. The attackers allegedly viewed that content on Facebook. The encouraging content ranged in specificity; for example, Fraenkel, although not a soldier, was kidnapped and murdered after Hamas members posted messages on Facebook that advocated the kidnapping of Israeli soldiers. The attack that killed the Braun baby at the light rail station in Jerusalem came after Hamas posts encouraged car-ramming attacks at light rail stations. By contrast, the killer of Force is alleged to have been a Facebook user, but plaintiffs do not set forth what specific content encouraged his

[4] When we refer to "Hamas" as users of Facebook in this opinion, we mean individuals alleged to be Hamas members or supporters, as well as various Hamas entities that are alleged to have Facebook pages.

attack, other than that "Hamas . . . use[d] Facebook to promote terrorist stabbings." App'x 335.

Hamas also used Facebook to celebrate these attacks and others, to transmit political messages, and to generally support further violence against Israel. The perpetrators were able to view this content because, although Facebook's terms and policies bar such use by Hamas and other designated foreign terrorist organizations, Facebook has allegedly failed to remove the "openly maintained" pages and associated content of certain Hamas leaders, spokesmen, and other members. App'x 229. It is also alleged that Facebook's algorithms directed such content to the personalized newsfeeds of the individuals who harmed the plaintiffs. Thus, plaintiffs claim, Facebook enables Hamas "to disseminate its messages directly to its intended audiences," App'x 255, and to "carry out the essential communication components of [its] terror attacks," App'x 256.

II. Facebook's Antiterrorism Efforts

A. Intended Uses of Facebook

Facebook has Terms of Service that govern the use of Facebook and purport to incorporate Facebook's Community Standards.[5] In its Terms of Service, Facebook represents that its services are intended to "[c]onnect you with people and organizations you care about," by, among other things, "[p]rovid[ing] a personalized experience" and "[h]elp[ing] you discover content, products, and services that may interest you." *Terms of Service*, Facebook, https://www.facebook.com/terms.php (last visited June 26, 2019). To

[5] Plaintiffs' complaint relies extensively on, and incorporates by reference, Facebook's Terms of Service and Community Standards (together, "terms"). The publicly available terms are also subject to judicial notice. *See* Fed. R. Evid. 201(b)(2); *see also, e.g., 23-34 94th St. Grocery Corp. v. N.Y.C. Bd. of Health*, 685 F.3d 174, 183 n.7 (2d Cir. 2012) (taking judicial notice of content of website whose authenticity was not in question). With the exception of such terms that plaintiffs allege Facebook actually follows in practice, we recount this information only for the limited purpose of setting forth Facebook's stated representations about its policies and practices and to provide context for plaintiffs' allegations, but not for the truth of whether Facebook follows those policies.

do so, Facebook "must collect and use your personal data," *id*., subject to a detailed "Data Policy," *Data Policy*, Facebook, https://www.facebook.com/about/privacy/update (last visited June 26, 2019). Facebook also uses information about its users to sell targeted online advertising and to provide advertisers with data on the effectiveness of their ads. *How do we use this information?*, *Data Policy*, Facebook, https://www.facebook.com/about/privacy/update (last visited May 23, 2019).

B. Prohibited Uses of Facebook

According to the current version of Facebook's Community Standards, Facebook "remove[s] content that expresses support or praise for groups, leaders, or individuals involved in," *inter alia*, "[t]errorist activity." *2. Dangerous Individuals and Organizations*, *Community Standards*, Facebook, https://www.facebook.com/communitystandards/dangerous_individuals_organizations (last visited June 26, 2019). "Terrorist

organizations and terrorists" may not "maintain a presence" on Facebook, nor is "coordination of support" for them allowed. *Id*. Facebook "do[es] not allow symbols that represent any [terrorist] organizations or [terrorists] to be shared on [the] platform without context that condemns or neutrally discusses the content." *Id*. In addition, Facebook purports to ban "hate speech" and to "remove content that glorifies violence or celebrates the suffering or humiliation of others." *Objectionable Content*, *Community Standards*, Facebook, https://www.facebook.com/communitystandards/objectionable_content (last visited June 26, 2019).

Facebook's Terms of Service also prohibit using its services "to do or share anything" that is, *inter alia*, "unlawful" or that "infringes or violates someone else's rights."[6] *Terms of Service*, *supra*. Violating

[6] Facebook's sign-up webpage states that by clicking "Sign Up," prospective users agree to Facebook's Terms of Service, Data Policy, and Cookies Policy—all of which are hyperlinked from that page. *Create a New Account*, Facebook, https://www.facebook.com/r.php (last visited June 26, 2019). As indicated above, the Terms of Service also purport to incorporate Facebook's Community Standards.

any of these policies may result in Facebook suspending or disabling a user's account, removing the user's content, blocking access to certain features, and contacting law enforcement. *Id*.

According to recent testimony by Facebook's General Counsel in a United States Senate hearing, Facebook employs a multilayered strategy to enforce these policies and combat extremist content on its platform.[7] Facebook claimed in the hearing that most of the content it removes is identified by Facebook's internal procedures before it is reported by users. For example, terrorist photos or videos that users attempt to upload are matched against an inventory of known terrorist content. Facebook is also experimenting with artificial intelligence to block or remove "text that might be advocating for terrorism." App'x 373. When Facebook detects terrorist-related content, it also uses artificial intelligence to identify similar, socially

[7] Plaintiffs included this testimony in the appendix on appeal and attached and referred to the testimony in their brief responding to the district court's order to show cause for why their proposed second amended complaint was not futile. We recount such testimony only for the purposes described *supra* n.5.

interconnected accounts, content, and pages that may themselves support terrorism.

The General Counsel also testified that, for content that is not automatically detected, Facebook employs thousands of people who respond to user reports of inappropriate content and remove such content. *Id.* Facebook also has a 150-person team of "counterterrorism specialists," including academics, engineers, and former prosecutors and law enforcement officers.[8] *Id*.

[8] Facebook has been criticized recently—and frequently—for not doing enough to take down offensive or illegal content. *E.g.*, Cecilia Kang, *Nancy Pelosi Criticizes Facebook for Handling of Altered Videos*, N.Y. Times (May 29, 2019), https://www.nytimes.com/2019/05/29/technology/facebook-pelosi-video.html; Kalev Leetaru, *Countering Online Extremism Is Too Important to Leave to Facebook*, FORBES (May 9, 2019), https://www.forbes.com/sites/kalevleetaru/2019/05/09/countering-online-extremism-is-too-important-to-leave-to-facebook; Julia Fioretti, *Internet Giants Not Doing Enough to Take Down Illegal Content: EU*, Reuters (Jan. 9, 2018), https://www.reuters.com/article/us-eu-internet-meeting/internet-giants-not-doing-enough-to-take-down-illegal-content-eu-idUSKBN1EY2BL; *see Staehr v. Harford Fin. Servs. Grp., Inc.*, 547 F.3d 406, 425 (2d Cir. 2008) ("[I]t is proper to take judicial notice of the *fact* that press coverage . . . contained certain information, without regard to the truth of their contents.").

III. District Court Proceeding

Plaintiffs brought this action on July 10, 2016, in the United States District Court for the Southern District of New York. On consent of the parties, the action was transferred to the United States District Court for the Eastern District of New York on September 16, 2016.[9] In their First Amended Complaint, Plaintiffs claimed that, under 18 U.S.C. § 2333, Facebook was civilly liable for aiding and abetting Hamas's acts of international terrorism; conspiring with Hamas in furtherance of acts of international terrorism; providing material support to terrorists; and providing material support to a designated foreign terrorist organization.[10] Plaintiffs also alleged that

[9] The parties moved jointly under 28 U.S.C. § 1404(a) to transfer the case to the Eastern District of New York because plaintiffs' counsel had already filed the *Cohen* action there, *see infra* n.11, and resolving both cases in the same district, the parties argued, would be efficient and convenient.

[10] 18 U.S.C. § 2333 provides civil remedies for injuries suffered through acts of international terrorism. Plaintiffs also cite to 18 U.S.C. § 2339A (providing material support for terrorism) and § 2339B (providing material support or resources to a designated foreign terrorist organization).

the district court had diversity-based subject matter jurisdiction under 28 U.S.C. § 1332(a)(2) to adjudicate Plaintiffs' Israeli-law tort claims arising from the same conduct.

Facebook moved to dismiss plaintiffs' claims for lack of personal jurisdiction under Rule 12(b)(2) and for failure to state a claim under Rule 12(b)(6). The district court determined that it had personal jurisdiction over Facebook, a ruling that Facebook does not challenge on appeal. But the district court also held that 47 U.S.C. § 230(c)(1) foreclosed plaintiffs' claims because they impermissibly involved "treat[ing]" Facebook "as the publisher or speaker of any information provided by" Hamas. S. App'x 18–23 (quoting 47 U.S.C. § 230(c)(1)).[11] On May 18, 2017, the district court granted the motion to dismiss under Rule 12(b)(6) and entered judgment in Facebook's

[11] In the same opinion, the district court also dismissed for lack of Article III standing the claims brought in a separate action by 20,000 Israeli citizens who, according to the district court, claimed "to be threatened only by potential future attacks." S. App'x 3. The district court referred to those plaintiffs as the "Cohen Plaintiffs" and to the plaintiffs in this appeal as the "Force Plaintiffs." *Id*. at 1. The Cohen Plaintiffs did not appeal. *Cohen v. Facebook*, 16-cv-04453-NGG-LB (E.D.N.Y.).

favor, without prejudice to plaintiffs seeking leave to file an amended complaint.

Plaintiffs then filed a Rule 59(e) motion to alter the judgment, asking the district court to reconsider its dismissal of their First Amended Complaint, and filed a motion seeking leave to file a second amended complaint. The proposed complaint retained all of plaintiffs' prior claims for relief and added a claim that Facebook had concealed its alleged material support to Hamas. In January 2018, the district court denied plaintiffs' motions with prejudice, holding that plaintiffs' proposed second amended complaint was futile in light of 47 U.S.C. § 230(c)(1). Plaintiffs timely appealed.

STANDARD OF REVIEW

Because the district court determined that it was futile to allow plaintiffs to file a second amended complaint, we evaluate that proposed complaint "as we would a motion to dismiss, determining whether [it] contains enough facts to state a claim to relief that is

plausible on its face."[12] *Ind. Pub. Ret. Sys. v. SAIC, Inc.*, 818 F.3d 85, 92 (2d Cir. 2016) (citation and internal quotation marks omitted). We accept as true all alleged facts in both the First Amended Complaint and the proposed second amended complaint.[13] *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). We also review *de novo* a district court's grant of a Rule 12(b)(6) motion to dismiss on the basis of an affirmative defense. *See Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 26 (2d Cir. 2015).

DISCUSSION

On appeal, plaintiffs contend that the district court improperly held that Section 230(c)(1) barred their claims. Plaintiffs argue that their claims do not treat Facebook as the "publisher" or "speaker" of

[12] We have jurisdiction over this appeal from a final judgment. 28 U.S.C. § 1291.

[13] Plaintiffs do not distinguish their arguments between their First Amended Complaint, which the district court dismissed, and their proposed second amended complaint, which the district court determined was futile. We agree that the Section 230(c)(1) issues raised by both complaints are materially indistinguishable.

content [14] provided by Hamas, as Section 230(c)(1) requires for immunity. Plaintiffs similarly contend that Facebook contributed to that content through its algorithms. Plaintiffs also argue that to apply Section 230(c)(1) to their claims based on Facebook's and Hamas's actions taken outside of the United States would constitute the unlawful extraterritorial application of that statute. In addition, plaintiffs maintain that 47 U.S.C. § 230(e)(1), which provides that Section 230 shall not be "construed to impair the enforcement of . . . any . . . Federal criminal statute," precludes the application of Section 230(c)(1) to their claims, that the Anti-Terrorism Act's ("ATA") civil remedies provision, 18 U.S.C. § 2333, irreconcilably conflicts with Section 230(c)(1), and that the Justice Against Sponsors of Terrorism Act ("JASTA") impliedly narrowed or repealed Section 230(c)(1). Lastly, plaintiffs contend that Section 230(c)(1) cannot apply to their

[14] We refer to "content" and "information" synonymously in this opinion.

claims brought under the foreign law of Israel.

In response to plaintiffs' claims, Facebook contends that Section 230(c)(1) provides it immunity and that, even absent such immunity, plaintiffs fail to plausibly allege that Facebook assisted Hamas in the ways required for their federal antiterrorism claims and Israeli law claims.

We first turn to the issues regarding Section 230(c)(1).[15]

I. Background of Section 230(c)(1)

The primary purpose of the proposed legislation that ultimately resulted in the Communications Decency Act ("CDA") "was to protect children from sexually explicit internet content." *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016) (citing 141

[15] Plaintiffs argue that the district court prematurely applied Section 230(c)(1), an affirmative defense, because discovery might show that Facebook was indeed a "developer" of Hamas's content. However, the application of Section 230(c)(1) is appropriate at the pleading stage when, as here, the "statute's barrier to suit is evident from the face of" plaintiffs' proposed complaint. *Ricci*, 781 F.3d at 28; *see also Marshall's Locksmith Serv. Inc. v. Google, LLC*, 925 F.3d 1263, 1267–68 (D.C. Cir. 2019) (affirming dismissal of claims at pleading stage based on Section 230(c)(1) immunity).

Cong. Rec. S1953 (daily ed. Feb. 1, 1995) (statement of Sen. Exon)). Section 230, though—added as an amendment to the CDA bill, *id.*—was enacted "to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum," *Ricci*, 781 F.3d at 28 (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997)). Indeed, Congress stated in Section 230 that "[i]t is the policy of the United States—(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; [and] (2) 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)(1)–(2).

In the seminal Fourth Circuit decision interpreting the immunity of Section 230 shortly after its enactment, *Zeran v. America Online, Inc.*, that court described Congress's concerns underlying Section 230:

> The amount of information communicated via interactive computer services is . . . staggering. The specter of . . . liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress . . . chose to immunize service providers to avoid any such restrictive effect.

129 F.3d at 331.

The addition of Section 230 to the proposed CDA also "assuaged Congressional concern regarding the outcome of two inconsistent judicial decisions," *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) and *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), both of which "appl[ied] traditional defamation law to internet providers," *LeadClick*, 838 F.3d at 173. As we noted in *LeadClick*, "[t]he first [decision] held that an interactive computer service provider could not be liable for a third party's defamatory statement . . . but the

second imposed liability where a service provider filtered its content in an effort to block obscene material." *Id.* (citations omitted) (citing 141 Cong. Rec. H8469-70 (daily ed. Aug. 4, 1995 (statement of Rep. Cox))).

To "overrule *Stratton*," *id*., and to accomplish its other objectives, Section 230(c)(1) provides 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."[16] 47 U.S.C. § 230(c)(1). Subject to certain delineated exceptions, *id*. § 230(e), Section 230(c)(1) thus shields a defendant from

[16] Section 230(c)(2), which, like Section 230(c)(1), is contained under the subheading "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material," 47 U.S.C. § 230(c), responds to *Stratton* even more directly. It provides that "[n]o provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [Section 230(c)(1)]." *Id.* § 230(c)(2).

civil liability when: (1) it is a "provider or user of an interactive computer service," as defined by § 230(f)(2); (2) the plaintiff's claims "treat[]" the defendant as the "publisher or speaker" of information, *id.* § 230(c)(1); and (3) that information is "provided by" an "information content provider," *id*. § 230(f)(3), other than the defendant interactive computer service.

In light of Congress's objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity. *See LeadClick*, 838 F.3d at 173 (collecting cases); *Marshall's Locksmith Serv. Inc. v. Google, LLC*, 925 F.3d 1263, 1267 (D.C. Cir. 2019) ("Congress inten[ded] to confer broad immunity for the re-publication of third-party content."); *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18 (1st Cir. 2016) ("There has been near-universal agreement that section 230 should not be construed grudgingly."); *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 408 (6th Cir. 2014) ("[C]lose cases . . . must be resolved in favor of

immunity.") (quoting *Fair Hous. Council v. Roommates.Com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc))); *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008) ("Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content."); *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted [Section 230] to establish broad . . . immunity.")); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003) ("§ 230(c) provides broad immunity for publishing content provided primarily by third parties.") (citation omitted); *Zeran*, 129 F.3d at 330 (4th Cir. 1997) ("Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.").

II. Whether Section 230(c)(1) Protects Facebook's Alleged Conduct[17]

The parties agree that Facebook is a provider of an "interactive computer service," but dispute whether plaintiffs' claims allege that (1) Facebook is acting as the protected publisher of information, and (2) the challenged information is provided by Hamas, or by Facebook itself.[18]

A. Whether Plaintiffs' Claims Implicate Facebook as a "Publisher" of Information

Certain important terms are left undefined by Section 230(c)(1),

---

[17] Because, as is discussed later in this opinion, plaintiffs' foreign law claims are dismissed on jurisdictional grounds, our discussion of Section 230(c)(1) immunity is confined to plaintiffs' federal claims.

[18] Plaintiffs also argue that because publication is not an explicit element of their federal anti-terrorism claims, Section 230(c)(1) does not provide Facebook with immunity. However, it is well established that Section 230(c)(1) applies not only to defamation claims, where publication is an explicit element, but also to claims where "the duty that the plaintiff alleges the defendant violated derives from the defendant's *status or conduct* as a publisher or speaker." *LeadClick*, 838 F.3d at 175 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009)) (emphasis added) (internal quotation marks omitted). "Thus, courts have invoked the prophylaxis of section 230(c)(1) in connection with a wide variety of causes of action, including housing discrimination, negligence, and securities fraud and cyberstalking." *Backpage.com*, 817 F.3d at 19 (internal citations omitted); *see also Marshall's Locksmith*, 925 F.3d at 1267 ("As courts uniformly recognize, § 230

including "publisher." 47 U.S.C. § 230(c)(1). This Circuit and others have generally looked to that term's ordinary meaning:[19] "one that makes public," *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014) (citing Webster's Third New International Dictionary 1837 (1981)); "the reproducer of a work intended for public consumption," *LeadClick*, 838 F.3d at 175 (citing *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009) (quoting Webster's Third New International Dictionary 1837 (Philip Babcock Gove ed., 1986))); and "one whose business is publication," *id.* Consistent with these definitions, in *Zeran v. America Online, Inc.*, the Fourth Circuit concluded that "[e]ven distributors are considered to be publishers," including "[t]hose who are in the business of making their facilities available to disseminate

immunizes internet services for third-party content that they publish, . . . against causes of action of all kinds."); *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 684 (9th Cir. 2019) ("[W]e have repeatedly held the scope of [Section 230] immunity to reach beyond defamation cases.").

[19] "When a term goes undefined in a statute, we give the term its ordinary meaning." *Taniguchi v. Kan Pac. Saipan, Ltd.*, 566 U.S. 560, 566 (2012).

. . . the information gathered by others." 129 F.3d at 332 (quoting W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 113, at 803 (5th ed. 1984)). The courts' generally broad construction of Section 230(c)(1) in favor of immunity "has resulted in a capacious conception of what it means to treat a website operator as the publisher . . . of information provided by a third party." *Backpage.com*, 817 F.3d at 19.

Plaintiffs seek to hold Facebook liable for "giving Hamas a forum with which to communicate and for actively bringing Hamas' message to interested parties." Appellants' Reply Br. 37; *see also, e.g.*, Appellants' Br. 50–51 (arguing that the federal anti-terrorism statutes "prohibit[] Facebook from supplying Hamas a platform and communications services"). But that alleged conduct by Facebook falls within the heartland of what it means to be the "publisher" of information under Section 230(c)(1). So, too, does Facebook's alleged failure to delete content from Hamas members' Facebook pages. *See*

LeadClick, 838 F.3d at 174 (stating that acting as the "publisher" under Section 230(c)(1) includes the decision whether to "withdraw" content).

Plaintiffs also argue that Facebook does not act as the publisher of Hamas's content within the meaning of Section 230(c)(1) because it uses algorithms to suggest content to users, resulting in "matchmaking." Appellants' Br. 51–52. For example, plaintiffs allege that Facebook's "newsfeed" uses algorithms that predict and show the third-party content that is most likely to interest and engage users. Facebook's algorithms also provide "friend suggestions," based on analysis of users' existing social connections on Facebook and other behavioral and demographic data. And, Facebook's advertising algorithms and "remarketing" technology allow advertisers to target ads to its users who are likely most interested in those ads.

We disagree with plaintiffs' contention that Facebook's use of algorithms renders it a non-publisher. First, we find no basis in the

ordinary meaning of "publisher," the other text of Section 230, or decisions interpreting Section 230, for concluding that an interactive computer service is not the "publisher" of third-party information when it uses tools such as algorithms that are designed to match that information with a consumer's interests.[20] *Cf., e.g., Roommates.Com*, 521 F.3d at 1172 (recognizing that Matchmaker.com website, which "provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs," was immune under Section 230(c)(1)) (citing *Carafano, Inc.*, 339 F.3d 1119); *Carafano*, 339 F.3d at 1124–25 ("Matchmaker's decision to structure the information provided by users allows the company to offer additional features, such as 'matching' profiles with similar characteristics . . . , [and such features] [a]rguably promote[] the expressed Congressional policy 'to promote the continued development of the Internet and other

[20] To the extent that plaintiffs rely on their undeveloped contention that the algorithms are "designed to radicalize," Appellants' Br. 51, we deem that argument waived. In addition, this allegation is not made in plaintiffs' complaints.

interactive computer services.' 47 U.S.C. § 230(b)(1)."); *Herrick v. Grindr, LLC*, 765 F. App'x 586, 591 (2d Cir. 2019) (summary order) ("To the extent that [plaintiff's claims] are premised on Grindr's [user-profile] matching and geolocation features, they are likewise barred . . . .").[21]

Indeed, arranging and distributing third-party information inherently forms "connections" and "matches" among speakers, content, and viewers of content, whether in interactive internet forums or in more traditional media.[22] That is an essential result of

[21] While lacking precedential value, "[w]e are, of course, permitted to consider summary orders for their persuasive value, and often draw guidance from them in later cases." *Brault v. Soc. Sec. Admin., Comm'r*, 683 F.3d 443, 450 n.5 (2d Cir. 2012).

[22] As journalist and author Tom Standage has observed, "[M]any of the ways in which we share, consume, and manipulate information, even in the Internet era, build upon habits and conventions that date back centuries." Tom Standage, *Writing on the Wall: Social Media – The First 2000 Years* 5 (2013). *See also* Tom Standage, *Benjamin Franklin, Social Media Pioneer*, Medium (Dec. 10, 2013), https://medium.com/new-media/benjamin-franklin-social-media-pioneer-3fb505b1ce7c ("Small and local, with circulations of a few hundred copies at best, [colonial] newspapers consisted in large part of letters from readers, and reprinted speeches, pamphlets and items from other papers. They provided an open platform through which people could share and discuss their views with others. They were, in short, social media.").

publishing. Accepting plaintiffs' argument would eviscerate Section 230(c)(1); a defendant interactive computer service would be ineligible for Section 230(c)(1) immunity by virtue of simply organizing and displaying content exclusively provided by third parties.

Plaintiffs' "matchmaking" argument would also deny immunity for the editorial decisions regarding third-party content that interactive computer services have made since the early days of the Internet. The services have always decided, for example, where on their sites (or other digital property) particular third-party content should reside and to whom it should be shown. Placing certain third-party content on a homepage, for example, tends to recommend that content to users more than if it were located elsewhere on a website. Internet services have also long been able to target the third-party content displayed to users based on, among other things, users' geolocation, language of choice, and registration information. And,

of course, the services must also decide what type and format of third-party content they will display, whether that be a chat forum for classic car lovers, a platform for blogging, a feed of recent articles from news sources frequently visited by the user, a map or directory of local businesses, or a dating service to find romantic partners. All of these decisions, like the decision to host third-party content in the first place, result in "connections" or "matches" of information and individuals, which would have not occurred but for the internet services' particular editorial choices regarding the display of third-party content. We, again, are unaware of case law denying Section 230(c)(1) immunity because of the "matchmaking" results of such editorial decisions.

Seen in this context, plaintiffs' argument that Facebook's algorithms uniquely form "connections" or "matchmake" is wrong. That, again, has been a fundamental result of publishing third-party content on the Internet since its beginning. Like the decision to place

third-party content on a homepage, for example, Facebook's algorithms might cause more such "matches" than other editorial decisions. But that is not a basis to exclude the use of algorithms from the scope of what it means to be a "publisher" under Section 230(c)(1). The matches also might—as compared to those resulting from other editorial decisions—present users with targeted content of even more interest to them, just as an English speaker, for example, may be best matched with English-language content. But it would turn Section 230(c)(1) upside down to hold that Congress intended that when publishers of third-party content become especially adept at performing the functions of publishers, they are no longer immunized from civil liability.[23]

[23] The dissent contends that our holding would necessarily immunize the dissent's hypothetical phone-calling acquaintance who brokers a connection between two published authors and facilitates the sharing of their works. *See* Dissent at 2. We disagree, for the simple reason that Section 230(c)(1) immunizes publishing activity only insofar as it is conducted by an "interactive computer service." Moreover, the third-party information must be "provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3).

Second, plaintiffs argue, in effect, that Facebook's use of algorithms is outside the scope of publishing because the algorithms *automate* Facebook's editorial decision-making. That argument, too, fails because "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific edit[orial] or selection process." *Carafano*, 339 F.3d at 1124; *see Marshall's Locksmith*, 925 F.3d at 1271 (holding that "automated editorial act[s]" are protected by Section 230) (quoting *O'Kroley v. Fastcase, Inc.*, 831 F.3d 352, 355 (6th Cir. 2016)); *cf., e.g., Roommates.Com*, 521 F.3d at 1172; *Herrick*, 765 F. App'x at 591. We disagree with plaintiffs that in enacting Section 230 to, *inter alia*, "promote the continued development of the Internet," 47 U.S.C. § 230(b)(1), and "preserve the vibrant and competitive free market," *id*. § 230(b)(2), Congress implicitly intended to restrain the automation of interactive computer services' publishing activities in order for them to retain immunity.

Our dissenting colleague calls for a narrow textual interpretation of Section 230(c)(1) by contending that the Internet was an "afterthought" of Congress in the CDA because the medium received less "committee attention" than other forms of media and that Congress, with Section 230, "tackled only . . . the ease with which the Internet delivers indecent or offensive material, especially to minors." Dissent at 5–6. But such a constrained view of Section 230 simply is not supported by the actual text of the statute that Congress passed. In addition to the broad language of Section 230(c)(1) and the pro-Internet-development policy statements in Section 230 (discussed *ante* at 24, 38), Congress announced the following specific findings in Section 230:

> (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
>
> (2) These services offer users a great degree of control over the information that they receive, as well as the

> potential for even greater control in the future as technology develops.
>
> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
>
> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

47 U.S.C. § 230(a)(1)–(5). These Congressional statements all point to the benefits of interactive media and "publisher" immunity to interactive computer services when they arrange and transmit information provided by others.

We therefore conclude that plaintiffs' claims fall within Facebook's status as the "publisher" of information within the meaning of Section 230(c)(1).

B. Whether Facebook is the Provider of the Information

We turn next to whether Facebook is plausibly alleged to *itself* be an "information content provider," or whether it is Hamas that provides all of the complained-of content. "The term 'information content provider' means 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). If Facebook was a creator or developer, even "in part," of the terrorism-related content upon which plaintiffs' claims rely, then Facebook is an "information content provider" of that content and is not protected by Section 230(c)(1) immunity. 47 U.S.C. § 230(f)(3). Plaintiffs contend that Facebook's algorithms "develop" Hamas's content by directing such content to users who are most interested in Hamas and its terrorist activities, without those

users necessarily seeking that content.

The term "development" in Section 230(f)(3) is undefined. However, consistent with broadly construing "publisher" under Section 230(c)(1), we have recognized that a defendant will not be considered to have developed third-party content unless the defendant directly and "materially" contributed to what made the content itself "unlawful." *LeadClick*, 838 F.3d at 174 (quoting *Roommates.Com*, 521 F.3d at 1168). This "material contribution" test, as the Ninth Circuit has described it, "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 v. Yelp! Inc.*, 836 F.3d 1263, 1269 n.4 (9th Cir. 2016) (quoting *Jones*, 755 F.3d at 413–14).

Employing this "material contribution" test, we held in *FTC v. LeadClick* that the defendant LeadClick had "developed" third parties'

content by giving specific instructions to those parties on how to edit "fake news" that they were using in their ads to encourage consumers to purchase their weight-loss products. *LeadClick*, 838 F.3d at 176. LeadClick's suggestions included adjusting weight-loss claims and providing legitimate-appearing news endorsements, thus "materially contributing to [the content's] alleged unlawfulness." *Id*. (quoting *Roommates.Com*, 521 F.3d at 1160) (alterations in the original). *LeadClick* also concluded that a defendant may, in some circumstances, be a developer of its users' content if it encourages or advises users to provide the specific actionable content that forms the basis for the claim. *See id.* Similarly, in *Fair Housing Council v. Roommates.Com*, 521 F.3d at 1172, the Ninth Circuit determined that—in the context of the Fair Housing Act, 42 U.S.C. § 3601 *et seq.*, which prohibits discrimination on the basis of sex, family status, sexual orientation, and other protected classes in activities related to housing—the defendant website's practice of requiring users to use

pre-populated responses to answer inherently discriminatory questions about membership in those protected classes amounted to developing the actionable information for purposes of the plaintiffs' discrimination claim.

Although it did not explicitly adopt the "material contribution" test, the D.C. Circuit's recent decision in *Marshall's Locksmith Service v. Google*, 925 F.3d 1263, illustrates how a website's display of third-party information does not cross the line into content development. There, "scam locksmiths"—who were apparently actual locksmiths seeking to mislead consumers with lock emergencies into believing that they were closer in proximity to the emergency location than they actually were—allegedly provided Google, Microsoft, and Yahoo!'s internet mapping services with false locations, some of which were exact street addresses and others which were "less-exact," such as telephone area codes. *Id*. at 1265–70. The internet mapping services of Google, Microsoft, and Yahoo! translated this information into

textual and pictorial "pinpoints" on maps that were displayed to the services' users. *Id*. at 1269. The D.C. Circuit concluded that this "translation" of the third-party information by the interactive computer services did not develop that information (or create new content) because the underlying "information [was] entirely provided by the third party, and the choice of *presentation*" fell within the interactive computer services' prerogative as publishers. *Id*. (emphasis added).

As to the "less-exact" location information, such as area codes, provided by the scam locksmiths, the plaintiffs also argued that the mapping services' algorithmic translation of this information into exact pinpoint map locations developed or created the misleading information. *Id*. at 1269–70. The D.C. Circuit also rejected that argument, holding that "defendants' translation of [imprecise] third-party information into map pinpoints does not convert them into 'information content providers' because defendants use a neutral

algorithm to make that translation." *Id*. at 1270. In using the term "neutral," the court observed that the algorithms were alleged to make no distinction between "scam" and other locksmiths and that the algorithms did not materially alter (i.e., they "hew[ed] to") the underlying information provided by the third parties. *Id*. at 1270 n.5, 1270–71.

Here, plaintiffs' allegations about Facebook's conduct do not render it responsible for the Hamas-related content. As an initial matter, Facebook does not edit (or suggest edits) for the content that its users—including Hamas—publish. That practice is consistent with Facebook's Terms of Service, which emphasize that a Facebook user "own[s] all of the content and information [the user] post[s] on Facebook, and [the user] can control how it is shared through [the user's] privacy and application settings." App'x 252.

Nor does Facebook's acquiring certain information from users render it a developer for the purposes of Section 230. Facebook

requires users to provide only basic identifying information: their names, telephone numbers, and email addresses. In so doing, Facebook acts as a "neutral intermediary." *LeadClick*, 838 F.3d at 174. Moreover, plaintiffs concede in the pleadings that Facebook does not publish that information, *cf., e.g., Roommates.Com*, 521 F.3d at 1172, and so such content plainly has no bearing on plaintiffs' claims.

Plaintiffs' allegations likewise indicate that Facebook's algorithms are content "neutral" in the sense that the D.C. Circuit used that term in *Marshall's Locksmith*: The algorithms take the information provided by Facebook users and "match" it to other users—again, materially unaltered—based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers.[24] Merely arranging and displaying others' content to users

[24] We do not mean that Section 230 requires algorithms to treat all types of content the same. To the contrary, Section 230 would plainly allow Facebook's algorithms to, for example, de-promote or block content it deemed objectionable. We emphasize only—assuming that such conduct could constitute "development" of third-party content—that plaintiffs do not plausibly allege that Facebook augments terrorist-supporting content primarily on the basis of its subject matter.

of Facebook through such algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook responsible as the "develop[er]" or "creat[or]" of that content. *See, e.g., Marshall's Locksmith*, 925 F.3d at 1269–71; *Roommates.Com*, 521 F.3d at 1169–70.

Plaintiffs' arguments to the contrary are unpersuasive. For one, they point to the Ninth Circuit's decision in *Roommates.Com* as holding that requiring or encouraging users to provide *any* particular information whatsoever to the interactive computer service transforms a defendant into a developer of that information. The *Roommates.Com* holding, however, was not so broad; it concluded only that the site's conduct in requiring users to select from "a limited set of pre-populated answers" to respond to particular "discriminatory questions" had a content-development effect that was actionable in the context of the Fair Housing Act. *See* 521 F.3d at 1166. There is no comparable allegation here.

Plaintiffs also argue that Facebook develops Hamas's content because Facebook's algorithms make that content more "visible," "available," and "usable." Appellants' Br. at 45–46. But making information more available is, again, an essential part of traditional *publishing*; it does not amount to "developing" that information within the meaning of Section 230. Similarly, plaintiffs assert that Facebook's algorithms suggest third-party content to users "based on what Facebook believes will cause the user to use Facebook as much as possible" and that Facebook intends to "influence" consumers' responses to that content. Appellants' Br. 48. This does not describe anything more than Facebook vigorously fulfilling its role as a publisher. Plaintiffs' suggestion that publishers must have no role in organizing or distributing third-party content in order to avoid "develop[ing]" that content is both ungrounded in the text of Section 230 and contrary to its purpose.

Finally, we note that plaintiffs also argue that Facebook should not be afforded Section 230 immunity because Facebook has chosen to undertake efforts to eliminate objectionable and dangerous content but has not been effective or consistent in those efforts. However, again, one of the purposes of Section 230 was to ensure that interactive computer services should not incur liability as developers or creators of third-party content merely because they undertake such efforts—even if they are not completely effective.[25]

We therefore conclude from the allegations of plaintiffs' complaint that Facebook did not "develop" the content of the Facebook postings by Hamas and that Section 230(c)(1) applies to Facebook's alleged conduct in this case.

III. Whether Applying Section 230(c)(1) to Plaintiffs' Claims Would Impair the Enforcement of a Federal Criminal Statute

Plaintiffs also argue that Section 230(c)(1) may not be applied

[25] *See supra*, Discussion, Part I.

to their claims because that would impermissibly "impair the enforcement" of a "Federal criminal statute." Appellant's Br. at 52 (quoting 47 U.S.C. § 230(e)(1)). Section 230(e)(1), entitled, "No effect on criminal law," is one of the enumerated exceptions to the application of Section 230(c)(1) immunity. It provides that "[n]othing in . . . section [230] shall be construed to impair the enforcement of . . . any [] Federal criminal statute." 47 U.S.C. § 230(e)(1). Plaintiffs observe that 18 U.S.C. §§ 2339A, 2339B, and 2339C, which criminalize providing material support for terrorism, providing material support for foreign terrorist organizations, and financing terrorism, respectively, are federal criminal statutes. Plaintiffs argue that preventing them from bringing an action under the statute providing for "civil remedies" for individuals injured "by reason of an act of international terrorism," 18 U.S.C. § 2333(a), would "impair the enforcement" of those criminal statutes within the meaning of 47 U.S.C. § 230(e)(1). In response, citing the First Circuit's decision in

Backpage.com, 817 F.3d at 23–24, Facebook argues that Section 230(e)(1) pertains only to criminal enforcement actions brought by a prosecutor, not civil actions such as this.

We agree with the district court's conclusion that Section 230(e)(1) is inapplicable in this civil action. Even accepting, *arguendo*, plaintiffs' assertion that a civil litigant could be said to "enforce" a criminal statute through a separate civil remedies provision, any purported ambiguity in Section 230(e)(1) is resolved by its title, "No effect on criminal law."[26] "Criminal law" concerns "prosecuting and punishing offenders" and is "contrasted with civil law," which, as here, concerns "private relations between individuals." *Criminal Law, Civil Law*, Oxford English Dictionary (3d ed. 2010). Furthermore, as the First Circuit pointed out in *Jane Doe No. 1 v. Backpage.com, LLC*, "where Congress wanted to include both civil and criminal remedies

[26] "[W]here the text is ambiguous, a statute's titles can offer 'a useful aid in resolving [the] ambiguity.'" *Lawson v. FMR LLC*, 571 U.S. 429, 465 (2014) (quoting *FTC v. Mandel Bros., Inc.*, 359 U.S. 385, 388–89 (1959) (alterations in original)).

in CDA provisions, it did so through broader language." 817 F.3d at 23. Section 230(e)(4), for example, states that Section 230 "should not 'be construed to limit the application of the Electronic Communications Privacy Act of 1986,' a statute that contains both criminal penalties and civil remedies." *Id.* (first quoting 18 U.S.C. § 230(e)(4), then citing 18 U.S.C. §§ 2511, 2520). In light of the presumption that the use of "different words within the same statutory scheme is deliberate," the fact that Congress's word choice in "[p]reserving the 'application' of this Act" is distinct from its "significantly narrower word choice in safeguarding the 'enforcement' of federal criminal statutes" counsels against the broad reading of Section 230(e)(1) urged by plaintiffs. *Id.* (citing *Sosa v. Alvarez-Machain*, 542 U.S. 692, 711 n.9 (2004)).[27] We therefore join the

[27] We do not here decide whether the word "enforcing" in a different provision, Section 230(e)(3), necessarily has the same meaning as "enforcement" in Section 230(e)(1), given their different linguistic contexts. *See* 47 U.S.C. § 230(e)(3) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section."); *Beharry v. Ashcroft*, 329 F.3d 51, 61 (2d Cir. 2003) (Sotomayor, *J.*) ("Usually identical words in different sections

First Circuit in concluding that Section 230(e)(1) is "quite clearly . . . limited to criminal prosecutions." *Backpage.com*, 817 F.3d at 23. Accordingly, Section 230(e)(1) provides no obstacle to the application of Section 230(c)(1) in this case.

IV. Whether the Anti-Terrorism Act's Civil Remedies Provision, 18 U.S.C. § 2333, Implicitly Narrowed or Repealed Section 230(c)(1)

Plaintiffs also argue that the ATA's civil remedies provision, 18 U.S.C. § 2333, irreconcilably conflicts with Section 230 and impliedly repealed it when Congress amended Section 2333 by adopting the Justice Against Sponsors of Terrorism Act ("JASTA") in 2016. JASTA, among other things, added civil liability for aiding and abetting and civil conspiracy to Section 2333, with a stated purpose of "provid[ing] civil litigants with the broadest possible basis . . . to seek relief" against material supporters of terrorism. Pub. L. 114–222,

---

mean identical things, but not invariably. All depends on context." (citation omitted)).

§ 2(b), 130 Stat. 852, 853 (2016).

"[R]epeals by implication are not favored and will not be presumed unless the intention of the legislature to repeal is clear and manifest." *Nat'l Ass'n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644, 662 (2007) (citation, internal quotation marks, and alterations omitted). In other words, "[a]n 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." *Branch v. Smith*, 538 U.S. 254, 273 (2003) (citation and internal quotation marks omitted). Here, there is no irreconcilable conflict between the statutes. Section 230 provides an affirmative defense to liability under Section 2333 for only the narrow set of defendants and conduct to which Section 230 applies. JASTA merely expanded Section 2333's cause of action to secondary liability; it provides no obstacle—explicit or implicit—to applying Section 230.

V. Whether Applying Section 230(c)(1) to Plaintiffs' Claims Would Be Impermissibly Extraterritorial

Plaintiffs also argue that the presumption against the extraterritorial application of federal statutes bars applying Section 230(c)(1) to their claims because Hamas posted content and conducted the attacks from overseas, and because Facebook's employees who failed to take down Hamas's content were allegedly located outside the United States, in Facebook's foreign facilities. In response, Facebook contends that Section 230(c)(1) merely limits civil liability in American courts, a purely domestic application.

Under the canon of statutory interpretation known as the "presumption against extraterritoriality," "[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 instructed courts to apply "a two-step framework for analyzing extraterritoriality issues." *Id*. at 2101. "At the first step,

we ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *Id*.

If the statute is not extraterritorial on its face, then "at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute's 'focus.'" *Id*. "The focus of a statute 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 LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2137 (2018) (citation, internal quotation marks, and alterations omitted). "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad . . . ." *RJR Nabisco*, 136 S. Ct. at 2101. "[B]ut if the conduct relevant to the focus occurred in a foreign country, then the

case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id*.

The two-step framework arguably does not easily apply to a statutory provision that affords an affirmative defense to civil liability. Indeed, it is unclear how an American court could apply such a provision "extraterritorially." Even if it could be applied extraterritorially—say, by somehow treating the defendant's conduct rather than the lawsuit itself as the "focus" of a liability-limiting provision—the presumption against extraterritoriality primarily "serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries." *Id*. at 2100. Allowing a plaintiff's claim to go forward because the cause of action applies extraterritorially, while then applying the presumption to block a different provision setting out defenses to that claim, would seem only to increase the possibility of international friction. Such a regime could also give plaintiffs an advantage when they sue over

extraterritorial wrongdoing that they would not receive if the defendant's conduct occurred domestically. It is doubtful that Congress ever intends such a result when it writes provisions limiting civil liability.

The Ninth Circuit addressed this issue in *Blazevska v. Raytheon Aircraft Co.*, 522 F.3d 948 (9th Cir. 2008), which was decided prior to the Supreme Court's adoption of the two-step extraterritoriality framework. The plaintiffs in *Blazevska* argued that the General Aviation Revitalization Act's ("GARA") statute of repose could not limit the defendant's liability because, like here, certain events related to plaintiffs' claims occurred overseas. *Id.* at 950. The Ninth Circuit disagreed, holding that the presumption against extraterritoriality was inapplicable to a liability-limiting statute. It found that GARA did not "impermissibly regulate conduct that has occurred abroad," and instead,

> merely eliminates the power of any party to bring a suit for damages against a general aviation aircraft

> manufacturer, in a U.S. federal or state court, after the limitation period. The only conduct it could arguably be said to regulate is the ability of a party to initiate an action for damages against a manufacturer in American courts—an entirely domestic endeavor. Congress has no power to tell courts of foreign countries whether they could entertain a suit against an American defendant.

Id. at 953. "Accordingly," the Ninth Circuit held, "the presumption against extraterritoriality simply is not implicated by GARA's application." *Id*.

The Supreme Court has left open the question of whether certain types of statutes might not be subject to the presumption against extraterritoriality. *See WesternGeco*, 138 S. Ct. at 2136 (noting, without deciding, the question whether "the presumption against extraterritoriality should never apply to statutes . . . that merely provide a general damages remedy for conduct that Congress has declared unlawful"). However, we need not decide here whether the presumption against extraterritoriality is "simply . . . not implicated,"*Blazevska*, 522 F.3d at 953, by statutes that merely limit

civil liability, or whether the two-step *RJR Nabisco* framework must be applied, because that framework is workable in this context and compels the same result. At step two, we conclude from the text of Section 230, particularly the words "shall be treated," that its primary purpose is limiting civil liability in American courts.[28] The regulated conduct—the litigation of civil claims in federal courts—occurs entirely domestically in its application here. We thus hold that the presumption against extraterritoriality is no barrier to the application of Section 230(c)(1) in this case.[29]

VI. Foreign Law Claims

Turning next to plaintiffs' foreign tort claims, the parties disagree as to the reach of Section 230 immunity. The district court

[28] Although "a finding of extraterritoriality at step one will obviate step two's 'focus' inquiry," courts may instead "start[] at step two in appropriate cases." *RJR Nabisco,* 136 S. Ct. at 2101 n.5.

[29] Because we conclude that the affirmative defense of Section 230(c)(1) applies, we need not reach Facebook's alternative argument that plaintiffs' complaint does not plausibly allege that, absent such immunity, Facebook assisted Hamas under the federal antiterrorism claims.

held that Section 230 applies to foreign law claims brought in United States courts, but it did not address the basis for its exercise of subject matter jurisdiction over those claims. Before we can reach the merits of those causes of action, including the applicability of Section 230, we must independently ensure the basis for federal subject matter jurisdiction. *Ruhrgas AG v. Marathon Oil Co.*, 526 U.S. 574, 583 (1999).

Plaintiffs allege that, under 28 U.S.C. § 1332(a)(2), we have diversity jurisdiction over their foreign law claims purportedly brought between "citizens of a State and citizens or subjects of a foreign state." It is well established, however, that "United States citizens who are domiciled abroad are neither citizens of any state of the United States nor citizens or subjects of a foreign state, and § 1332(a) does not provide that the courts have jurisdiction over a suit to which such persons are parties." *Cresswell v. Sullivan & Cromwell*, 922 F.2d 60, 68 (2d Cir. 1990). In other words, "a suit by or against United States citizens domiciled abroad may not be premised on

diversity." *Id.*; *see also Newman-Green, Inc. v. Alfonzo-Larrain*, 490 U.S. 826, 829 (1989) (stating that "stateless" United States citizens may not be parties to diversity-based suits).

Here, a substantial majority of the plaintiffs are alleged to be United States citizens domiciled in Israel.[30] A suit based on diversity jurisdiction may not proceed with these plaintiffs as parties.

In addition, "[i]t is well established that for a case to come within [§ 1332] there must be complete diversity," *Cresswell*, 922 F.2d at 68, and the complaint must set forth the citizenship of the parties, *Leveraged Leasing Admin. Corp. v. PacifiCorp Capital, Inc.*, 87 F.3d 44, 47 (2d Cir. 1996). Plaintiffs' complaint fails to allege the state citizenship, if any, of U.S.-citizen plaintiffs Taylor Force, Kristin Ann Force, Yaakov Naftali Fraenkel, Chaya Zissel Braun, Richard Lakin, or the minor-children plaintiffs S.S.R., M.M.R., R.M.R. and S.Z.R. We thus cannot determine on the present record whether those plaintiffs are

[30] A representative of a decedent's estate is "deemed to be a citizen only of the same State as the decedent." 28 U.S.C. § 1332(c)(2).

of diverse citizenship from Facebook. Indeed, only *two* plaintiffs—Stuart Force and Robbi Force—are alleged to be of diverse citizenship to Facebook.

The joinder of Israel-domiciled U.S.-citizen plaintiffs requires us either to dismiss the diversity-based claims altogether, or exercise our discretion to: 1) dismiss those plaintiffs who we determine are "dispensable jurisdictional spoilers;" or 2) vacate in part the judgment of the district court and remand for it to make that indispensability determination and to determine whether dismissal of those individuals would be appropriate. *SCS Commc'ns, Inc. v. Herrick Co.*, 360 F.3d 329, 335 (2d Cir. 2004). As for the plaintiffs for whom no state citizenship is alleged, we have discretionary authority to accept submissions for the purpose of amending the complaint on appeal, or we could remand for amendment. *See Leveraged Leasing*, 87 F.3d at 47 ("Defective allegations of jurisdiction may be amended, upon terms, in the trial or appellate courts." (quoting 28 U.S.C. § 1653)).

We decline to exercise our discretion to attempt to remedy these jurisdictional defects. This is not a case in which a small number of nondiverse parties defeats jurisdiction, but rather one in which—after multiple complaints have been submitted—most of the plaintiffs are improperly joined. Moreover, the case remains at the pleading stage, with discovery not yet having begun. Proceeding with the few diverse plaintiffs would be inefficient given the expenditure of judicial and party resources that would be required to address the jurisdictional defects. The most appropriate course is for any diverse plaintiffs to bring a new action and demonstrate subject matter jurisdiction in that action.[31] Accordingly, plaintiffs' foreign law

[31] Plaintiffs do not assert supplemental jurisdiction under 28 U.S.C. § 1367. All claims over which we have original jurisdiction are dismissed at the pleading stage, *see id*. § 1367(c)(3), and, by plaintiffs' own argument, some of the foreign claims "differ[] markedly from American concepts of . . . liability," Appellants' Br. 59; *see id*. § 1367(c)(1). Therefore, even assuming that plaintiffs' foreign law claims form "part of the same case or controversy" as their federal claims, 28 U.S.C. § 1367(a), we decline to exercise supplemental jurisdiction here.

claims are dismissed, without prejudice.[32]

CONCLUSION

For the foregoing reasons, we **AFFIRM** the judgment of the district court as to plaintiffs' federal claims and **DISMISS** plaintiffs' foreign law claims.

[32] Because plaintiffs' foreign law claims are dismissed on jurisdictional grounds, we express no opinion as to the district court's conclusion that Section 230 applies to foreign law claims brought in United States courts.

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.").