934 F.3d 53
United States Court of Appeals, Second Circuit.

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]
No. 18-397
|
August Term, 2018
|
Argued: February 25, 2019
|
Decided: July 31, 2019

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

Attorneys and Law Firms

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.

Before: Katzmann, Chief Judge, Droney, and Sullivan, Circuit Judges.

---

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

Opinion

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

---

[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.

and 2016. Yaakov Naftali Fraenkel, a teenager, was kidnapped by a Hamas operative in 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]

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

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

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 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

---

[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.

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 do so,

[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.

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 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

---

[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.

[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.

intelligence to identify similar, socially 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*.

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,

---

[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. Hartford 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.").

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 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. *Cohen v. Facebook, Inc.*, 252 F.Supp.3d 140, 155–58 (E.D.N.Y. 2017) (quoting 47

---

[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).

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 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]

---

[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.).

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, 129 S.Ct. 1937, 173 L.Ed.2d 868 (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 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

---

[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.

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

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 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]

---

[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).

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 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. H8469-70141 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 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

---

[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).

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

[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.

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), 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

---

[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 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, 132 S.Ct. 1997, 182 L.Ed.2d 903 (2012).

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 . . . 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

[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.

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 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

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

---

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.").

"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 76. We

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

---

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).

the Internet delivers indecent or offensive material, especially to minors." Dissent at 78. 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 *supra* at 63, 67), 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 of Facebook through such algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook

---

[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, demote 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.

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 prepopulated 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 to their claims because that would impermissibly "impair the enforcement" of a "Federal criminal statute." Appellant's Br. at 52 (quoting 47

---

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

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"

---

[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, 134 S.Ct. 1158, 188 L.Ed.2d 158 (2014)

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 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, 124 S.Ct. 2739, 159 L.Ed.2d 718 (2004)).[27]

(quoting *FTC v. Mandel Bros., Inc.*, 359 U.S. 385, 388-89, 79 S.Ct. 818, 3 L.Ed.2d 893 (1959) (alterations in original)).

[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

We therefore join the 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, § 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, 127 S.Ct. 2518, 168 L.Ed.2d 467 (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

---

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

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, 123 S.Ct. 1429, 155 L.Ed.2d 407 (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., ___ U.S. ___, 136 S. Ct. 2090, 2100, 195 L.Ed.2d 476 (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.*, ___ U.S. ___, 138 S. Ct. 2129, 2137, 201 L.Ed.2d 584 (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 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, 119 S.Ct. 1563, 143 L.Ed.2d 760 (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

---

[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.

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, 109 S.Ct. 2218, 104 L.Ed.2d 893 (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

---

[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).

S.Z.R. We thus cannot determine on the present record whether those plaintiffs are 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 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.

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

---

[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.

[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.

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 71-72. 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, 117 S.Ct. 2329, 138 L.Ed.2d 874 (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 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

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 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).

---

§ 230(e)(1) as allowing for civil enforcement by, among others, the FCC, even if only in aid of criminal law enforcement.

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, 117 S.Ct. 2329. 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, 117 S.Ct. 2329. 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 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 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, 117 S.Ct. 2329.[2] The Supreme Court promptly struck down two major provisions of the Exon Amendment as unconstitutionally overbroad under the First Amendment, leaving the new § 230 as

[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)).

the dominant force for securing decency on the Internet. *See Reno*, 521 U.S. at 849, 117 S.Ct. 2329.

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 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 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 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

---

[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 63. 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).

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] 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.

---

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

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 65, 66, 70. 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*, ___ U.S. ___, 139 S. Ct. 954, 965, 203 L.Ed.2d 333 (2019) (citation and internal quotation marks omitted). 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, 930 F.3d 136, 153–54, 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*, 930 F.3d at 151, 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,

[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.

Facebook's suggestions contribute to the 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 70, 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

---

[6] *See*, *e.g.*, Gregory Waters & Robert Postings, *Spiders of the Caliphate: Mapping the Islamic State's Global Support*

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 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,

---

Network on Facebook 8, Counter Extremism Project (May 2018), http://www.counterextremism.com/sites/default/files/Spiders%20***o***f%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.

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* [sic] *to Reach*

'*Jew Haters*,' ProPublica (Sept. 14, 2017), https://www.propublica.org/article/facebookenabled-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 PresidentialElection* 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, *RadicalIdeas 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

---

[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* [sic] *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;

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 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,

---

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.

which acted as a digital bulletin board and did nothing proactive to forge off-site connections.[8]

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

---

[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"; 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").

the legal academy[9] and in the policy 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

---

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

[10] *See*, *e.g.*, Tarleton Gillespie, *How Social Networks 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.").

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.

304 F.Supp.3d 315
United States District Court, E.D. New York.

Stuart FORCE, individually and as Administrator on behalf of the Estate of Taylor Force, et al., Plaintiffs,
v.
FACEBOOK, INC., Defendant.

16-CV-5158 (NGG) (LB)
|
Signed January 17, 2018
|
Filed 01/18/2018

Attorneys and Law Firms

Robert Joseph Tolchin, The Berkman Law Office, LLC, Brooklyn, NY, for Plaintiffs.

Kenneth W. Allen, Craig S. Primis, Pro Hac Vice, Kirkland & Ellis LLP, Washington, DC, Paul S. Grewal, Facebook, Inc., Menlo Park, CA, Shireen Anneke Barday, Thomas Aulden Burcher-DuPont, Kirkland & Ellis LLP, New York, NY, for Defendant.

MEMORANDUM & ORDER

NICHOLAS G. GARAUFIS, United States District Judge

Plaintiffs in the above-captioned action are the victims, estates, and family members of victims of terrorist attacks in Israel. (1st Am. Compl. ("FAC") (Dkt. 28).) They assert various claims against Facebook, Inc. ("Facebook") based on their contention that Facebook

has supported the terrorist organization Hamas by allowing that group and its members and supporters to use Facebook's social media platform to further their aims.

On May 18, 2017, the court dismissed Plaintiffs' first amended complaint without prejudice for failure to state a claim upon which relief may be granted.[1] (May 18, 2017, Mem. & Order ("May 18 M & O") (Dkt. 48).) Before the court are Plaintiffs' motions to alter the judgment dismissing the first amended complaint (Mot. to Alter J. ("Recons. Mot.") (Dkt. 50)) and for leave to file a second amended complaint (Mot. for Leave to File 2d Am. Compl. ("Amendment Mot.") (Dkt. 52)). For the following reasons, the court DENIES both motions.

I. BACKGROUND

The court assumes familiarity with Plaintiffs' allegations and the court's prior decision granting Facebook's motion to dismiss Plaintiffs' first amended complaint. (*See* May 18 M & O.) In that opinion, the court specified that the dismissal was without prejudice. (*Id.* at 28.) On June 15, 2017, Plaintiffs filed two motions: first, a motion to alter the judgment, "retracting [the May 18 M & O] and issuing a modified opinion denying Facebook's motion to dismiss" (Recons. Mot.); and second, a motion for leave to file a second amended

[1] In that order, the court also addressed the factually similar allegations in *Cohen v. Facebook, Inc.*, No. 16-CV-4453, and dismissed the operative complaint in that case as well. (May 18 M & O.)

complaint, a copy of which Plaintiffs appended to their memorandum in support of that motion (Amendment Mot.; *see also* Proposed 2d Am. Compl. ("PSAC") (Dkt. 53-1)).

II. DISCUSSION

A. Motion to Alter the Judgment

Plaintiffs ask the court to reconsider its dismissal of the first amended complaint. The court concluded that all of the claims contained therein were barred by Section 230(c)(1) ("Section 230") of the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1). That law 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). Examining the myriad opinions considering the application of that law, the court concluded that each of Plaintiffs' claims and theories of liability sought to hold Facebook liable based on its role as the "publisher or speaker" of social media content generated by Hamas and affiliated individuals, and so were barred by the defense afforded by Section 230. (May 18 M & O at 17-23.) The court also held that applying Section 230 to the claims and theories at issue did not require an impermissible extraterritorial application of the CDA, as the relevant location for its extraterritoriality analysis was "the situs of the litigation." (*Id.* at 26.)

Plaintiffs contend that the court erred both in its determination that Section 230 applied to the claims

raised in the first amended complaint and that the application of that law to those claims was not impermissibly extraterritorial. They seek reconsideration and rescission of the opinion dismissing their complaint pursuant to Rule 59(e) of the Federal Rules of Civil Procedure. For the reasons that follow, the court sees no reason to reconsider its previous decision dismissing the first amended complaint.

1. Legal Standard

"A motion for reconsideration should be granted only when the [moving party] identifies 'an intervening change of controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice.'" *Kolel Beth Yechiel Mechil of Tartikov, Inc. v. YLL Irrevocable Tr.,* 729 F.3d 99, 104 (2d Cir. 2013) (quoting *Virgin Atl. Airways v. Nat'l Mediation Bd.,* 956 F.2d 1245, 1255 (2d Cir. 1992)). "It is well-settled that Rule 59 is not a vehicle for relitigating old issues, presenting the case under new theories, securing a rehearing on the merits, or otherwise taking a 'second bite at the apple.'" *Analytical Surveys, Inc. v. Tonga Partners, L.P.,* 684 F.3d 36, 52 (2d Cir. 2012) (internal quotation marks and citation omitted). "[T]he standard for granting a Rule 59 motion for reconsideration is strict, and reconsideration will generally be denied unless the moving party can point to controlling decisions or data that the court overlooked." *Id.* (quoting *Shrader v. CSX Transp., Inc.,* 70 F.3d 255, 257 (2d Cir. 1995)) (alterations omitted). "The burden is on the movant to demonstrate that the Court overlooked

controlling decisions or material facts that were before it on the original motion and that might materially have influenced its earlier decision." *Schoolcraft v. City of New York,* 248 F.Supp.3d 506, 508 (S.D.N.Y. 2017); *see also Levin v. Gallery 63 Antiques Corp.,* No. 04-CV-1504 (KMK), 2007 WL 1288641, at *2 (S.D.N.Y. Apr. 30, 2007) ("Motions for reconsideration allow the district court to correct its own mistakes, not those of the Parties." (internal quotation marks and citations omitted)).

2. Application

Plaintiffs argue that the court erred in (1) determining that the "focus" of Section 230 was on the "limitation of liability;" and (2) applying Section 230 to the claims against Facebook and, particularly, to claims raised under the Anti-Terrorism Act ("ATA") and Israeli law. (*See generally* Mem. in Supp. of Mot. for Recons. ("Recons. Mem." (Dkt. 51).)) The court addresses these arguments in turn.

a. "Focus" of Section 230

Plaintiffs first argue that the court erred in concluding that the presumption against extraterritoriality did not preclude application of Section 230 to the allegations raised in the first amended complaint. Plaintiffs take particular issue with the court's determination that Section 230's "focus" was on that section's "limitation on liability." (Recons. Mem. at 4 (quoting May 18 M & O at 25).) Plaintiffs argue both

that the court's identification of the statutory "focus" was based on an overly narrow focus on the provision at issue in this litigation, Section 230(c)(1) (Recons. Mem. at 4-5), and that the court's conclusion that the statute's focus is on liability "wrongly conflates the effect of a statute with its focus," which is on the actions of interactive computer providers (*id.* at 5-8).

Plaintiffs' arguments on this point do not come close to meriting reconsideration. The court notes that Plaintiffs at no point attempted to raise either of these arguments in their opposition to Facebook's motion to dismiss; in fact, the portions of Plaintiffs' brief discussing extraterritoriality do not even mention the word "focus." (*See* Pls. Mem. in Opp'n to Mot. to Dismiss ("Pls. MTD Opp'n") (Dkt. 40) at 30-31.) Plaintiffs provide no reason why they could not have presented such arguments in their initial briefing, and such new arguments have no place in a motion for reconsideration. *See, e.g.*, *Schoolcraft,* 248 F.Supp.3d at 508. While Plaintiffs now seek to take a new tack, "[a] party requesting reconsideration is not supposed to treat the court's initial decision as the opening of a dialogue in which that party may then use Rule [59(e)] to advance new facts and theories in response to the court's rulings." *Id.* at 509 (quoting *Church of Scientology Int'l v. Time Warner, Inc.,* No. 92-CV-3024 (PKL), 1997 WL 538912, at *2 (S.D.N.Y. Aug. 27, 1997)).

Moreover, Plaintiffs identify no contrary authority that the court overlooked or misapplied, as is normally required to obtain reconsideration. *See Analytical Surveys,* 684 F.3d at 52. Instead, Plaintiffs contend the

court's approach is generally at odds with Supreme Court and Second Circuit opinions examining issues of extraterritoriality because the court failed to adequately account for "statutory context." (Recons. Mem at 4-6.) Plaintiffs plainly misread the court's opinion, however, which was explicit in basing its conclusion about the statute's focus on its reading of Section 230 as a whole. (*See* May 18 M & O at 25-26 (examining policy statements and substantive provisions of Section 230).)

Plaintiffs' second argument—that the court's holding that Section 230's focus is on limiting liability "wrongly conflates the effect of a statute with its focus" (Recons. Mem. at 6-7) —is likewise unsupported by any contrary authority. Plaintiffs wave their hands at two recent Supreme Court decisions contemplating statutes *other* than the CDA and purport to draw from those decisions the proposition that "no statute's focus can ever be to simply limit liability." (*Id.* at 6-7 (citing *Morrison v. Nat'l Austl. Bank Ltd.,* 561 U.S. 247, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010), and *Kiobel v. Royal Dutch Petroleum Co.,* 569 U.S. 108, 133 S.Ct. 1659, 185 L.Ed.2d 671 (2013)).) However, those decisions offer no support for such a broad generalization, as they examine only the particular statutes before the Court while stressing that the touchstone of extraterritoriality analysis must be on the "focus of congressional concern" in enacting the challenged statute. *Morrison,* 561 U.S. at 266, 130 S.Ct. 2869. The court sees nothing in those opinions that disturbs its analysis of the CDA and certainly sees nothing that suggests that

Congress's focus in enacting a statute can *never* be on limiting liability.

b. The Scope of the CDA

Plaintiffs next argue that the court misapplied Section 230 to their claims against Facebook. (Recons. Mem. at 8-17.) Plaintiffs make two separate arguments: first, that the court failed to consider Plaintiffs' allegations and arguments that Facebook acted as an "information content provider," independent of content provided by Hamas-affiliated users (*id.* at 11-14); and second, that the court incorrectly extended Section 230's coverage to "valuable services" provided by Facebook (*id.* at 14-17). The court examines these arguments separately.

i. Facebook's Role as "Information Content Provider"

Plaintiffs first contend that the court failed to address their contention that Facebook acted as an "information content provider" within the meaning of Section 230 and could not claim protection under that section. As noted in the court's original decision, the protection afforded by Section 230 applies only to claims "based on information provided by [an] information content provider" other than the defendant. (May 18 M & O at 18-19 (quoting *FTC v. LeadClick Media, LLC,* 838 F.3d 158, 173 (2d Cir. 2016)).) Plaintiffs now maintain that their claims have, in fact, always sought to hold Facebook liable for its own content, and not that generated by another "information content

provider," *i.e.* Hamas and related entities, based on Facebook's alleged role in "networking" and "brokering" links among terrorists. (Recons. Mot. at 12.)

Plaintiffs' contention is completely disingenuous. In the current motion, Plaintiffs acknowledge in a footnote that "perhaps plaintiffs could have made their reliance on Facebook's productive conduct clearer in their briefing" but attribute this oversight to Facebook's supposed failure to argue that it was not a content provider. (Recons. Mot. at 12 & n.9.) Plaintiffs' contention is flatly refuted by Facebook's briefing on the original motion to dismiss, which clearly argued that all of the offending content cited in Plaintiffs' complaint was "provided by another information content provider, not by Facebook itself." (Def. Mem. in Supp. of MTD (Dkt. 35) at 17-18.) Plaintiffs did not respond to this argument at any point, and in fact *began* their opposition memorandum by stating that "[t]hese cases do not concern speech or content." (Pls. MTD Opp'n at 1.) For Plaintiffs to now turn around and argue that its allegations are largely about content that Facebook itself created borders on mendacious. More to the point, this entirely new argument in support of liability is not suitably considered on a motion for reconsideration, which "may not be used to advance new facts, issues or arguments not previously presented to the Court." *See Montblanc-Simplo GmbH v. Colibri Corp.*, 739 F.Supp.2d 143, 147 (E.D.N.Y. 2010) (internal quotation marks and citations omitted).

ii. Facebook's Conduct as "Speaker or Publisher"

Plaintiffs next contend that the court "misapprehended" the scope of their claims in failing to consider Plaintiffs' allegation that Facebook "provided . . . terrorists with valuable services unrelated to publication . . . that do not fall within the traditional role of a publisher." (Recons. Mem. at 16.) In particular, Plaintiffs contend that they are suing Facebook for "developing, encouraging, and facilitating connections between terrorists," and not simply based on its failure to "police its accounts" and remove terrorist-affiliated users. (*Id.*)

In the court's view, however, it has already addressed Plaintiffs' argument and need not revisit its conclusions on that point. It is true that the court's previous opinion focused largely on whether Facebook's provision of accounts to Hamas-affiliated users could meaningfully be separated from its role as a "publisher or speaker" of content produced by users, with the court concluding that "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally "derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'" (May 18 M & O at 21 (quoting *LeadClick Media*, 838 F.3d at 175).) While Plaintiffs now seek to distinguish between "making [Facebook's] system available to terrorists and a terrorist organization" and "provid[ing] [] terrorists with valuable services" through such access (Recons. Mem. at 16), this is a distinction without a difference: the "valuable services" at issue are part and parcel of

access to a Facebook account, and so imposing liability on that basis would again effectively turn on "Facebook's choices as to who may use its platform." (May 18 M & O at 21.) Plaintiffs are merely attempting to rehash arguments that the court has already considered and rejected, which are insufficient to merit reconsideration.[2] *See Shrader*, 70 F.3d at 257 ("[A] motion to reconsider should not be granted where the moving party seeks solely to relitigate an issue already decided.").

c. Interplay Between the CDA and the ATA

Plaintiffs next argue that, even if Section 230 would otherwise apply to the challenged conduct, it cannot apply here because such application "would be in direct conflict with the ATA." (Recons. Mem. at 19.) Though presented in several ways, Plaintiffs' essential argument is two part: (1) the ATA's goal of imposing expansive civil liability for harms resulting from terrorism is at odds with immunity under Section 230;

---

[2] Plaintiffs make the related argument that the court simply erred in its conclusion that Section 230 protects Facebook from liability based on its provision of user accounts and platform services to Hamas-affiliated users. (Recons. Mem. at 17-18.) However, Plaintiff provides no contrary controlling authority, but only argues the court unduly expanded the scope of Section 230's coverage beyond that envisioned by the Second Circuit. (*Id.* at 18.) As with Plaintiffs' more indirect attack on the court's holding discussed above, the court sees no reason to permit relitigation of issues already decided simply because Plaintiffs are dissatisfied with the court's prior decision.

and (2) because the ATA was adopted and amended after the CDA, it supersedes Section 230. (*Id.* at 17-23.)

At the outset, the court notes that it is skeptical that this argument is properly raised in the instant motion, as it can hardly be said to have been fully presented previously. Plaintiffs first advanced this argument in a single line in a footnote in their brief opposing Facebook's motion to dismiss. (See Pls. MTD Opp'n at 27 n.6 ("Even if there were a conflict between the limited immunity granted by the CDA and the liability imposed by the ATA, the ATA would control as its later enactment would be a tacit limiting of the CDA.").) Expanding this line to encompass five pages of their present briefing seems to the court to be the very definition of impermissibly "advanc[ing] . . . arguments not previously presented to the court." *Schoolcraft,* 248 F.Supp.3d at 508 (internal quotation marks and citations omitted).

Even if Plaintiffs' argument is not waived, however, it is meritless. Quoting from the preamble to the most recent amendment to the ATA, Plaintiffs contend that immunizing Facebook under Section 230 frustrates Congress's purpose of "provid[ing] civil litigants with the broadest possible basis . . . to seek relief against entities . . . that have provided material support, whether directly or indirectly, to foreign organizations or persons that engage in terrorist activities."[3]

---

[3] While it is not necessary to the decision here, the court notes that, whatever their interpretive value, statements of purpose contained in the preamble to a statute are not part of the

(Recons. Mem. at 21 (quoting Justice Against Sponsors of Terrorism Act ("JASTA"), § 2(b), Pub. L. No. 114-222, 130 Stat. 852, 853).) Plaintiffs do not suggest that the ATA explicitly limits Section 230 immunity, however, but instead argue that the ATA's later-in-time enactment and the broad policy statements quoted above implicitly displace Section 230 with respect to ATA-based civil actions. (*Id.* at 21-23.)

"When it is claimed that a later enacted statute creates an irreconcilable conflict with an earlier statute, the question is whether the later statute, by implication, has repealed all or, more typically, part of the earlier statute." *Garfield v. Ocwen Loans Servicing, LLC,* 811 F.3d 86, 89 (2d Cir. 2016). "[R]epeals by implication are not favored." *In re Stock Exch. Options Trading Antitrust Litig.,* 317 F.3d 134, 144 (2d Cir. 2003) (quoting *United States v. Borden Co.,* 308 U.S. 188, 198, 60 S.Ct. 182, 84 L.Ed. 181 (1939)). Accordingly, courts must not "infer a statutory repeal unless the later statute expressly contradicts the original act or unless such construction is absolutely necessary in order that the words of the later statute shall have any meaning at all." *Nat'l Ass'n of Home Builders v. Defenders of Wildlife,* 551 U.S. 644, 662, 127 S.Ct. 2518, 168 L.Ed.2d 467 (2007) (internal quotation marks and citations omitted, and alterations omitted); *see also Radzanower v. Touche Ross & Co.,* 426 U.S. 148, 155, 96 S.Ct. 1989, 48 L.Ed.2d 540 (1976) ("The statutory provisions at issue here cannot be said to be in

---

substantive scope of the law itself. *See, e.g.,* 73 Am. Jur. 2d Statutes § 101 (2d ed. updated Nov. 2017).

'irreconcilable conflict' in the sense that there is a positive repugnancy between them or that they cannot mutually co-exist."). "[A] statute dealing with a narrow, precise, and specific subject is not submerged by a later enacted statute covering a more generalized spectrum." *Nat'l Ass'n of Home Builders,* 551 U.S. at 663, 127 S.Ct. 2518 (quoting *Radzanower,* 426 U.S. at 153, 96 S.Ct. 1989).

The court sees no reason to conclude that the ATA impliedly abrogated Section 230, as each statute can be enforced without depriving the other of "any meaning at all." *Id.* at 662, 127 S.Ct. 2518. The ATA's civil recovery provisions create a broad right of recovery for U.S. nationals injured by acts of international terrorism, without differentiating based on the particular defendants against whom claims are raised. 18 U.S.C. § 2333. In enacting Section 230, however, Congress "was focusing on the particularized problems of [providers and users of interactive computer services] that might be sued in the state or federal courts," *Radzanower,* 426 U.S. at 153, 96 S.Ct. 1989, limiting the liability of a narrow subset of defendants for a particular type of claims. Thus, the ATA's general cause of action for victims of international terrorism cannot be said to "expressly contradict[ ]" the CDA, nor does the Section 230's limitation on certain theories of liability deprive the ATA of "any meaning at all." *Nat'l Ass'n of Home Builders,* 551 U.S. at 662, 127 S.Ct. 2518. Said differently, the two acts can be read without any conflict: Section 230 provides a limited defense to a specific

subset of defendants against the liability imposed by the ATA.

In contrast to the direction provided by the Supreme Court and Second Circuit to act cautiously in inferring statutory repeal, Plaintiffs urge an approach that would treat *any* statute that imposes liability and which was enacted after the CDA as implicitly limiting the reach of Section 230 absent an affirmative contrary statement. This approach would effectively reverse the presumption against inferring repeal and is patently inconsistent with the law outlined above.[4]

Accordingly, the court sees no reason to conclude that the ATA implicitly limited or repealed Section 230 or any other part of the CDA or to reconsider its prior opinion on that basis.

d. Application of the CDA to Plaintiffs' Israeli Law Claims

Plaintiffs' final argument is that the court erred in applying Section 230 to Plaintiffs' Israeli-law claims. (Recons. Mem. at 24-25.) Plaintiffs argue that court should have conducted a conflict-of-laws analysis, which would have demonstrated that Israeli (as opposed to New York) law applied to a number of

---

[4] Plaintiffs make the related argument that the court's interpretation of Section 230 "yields results that can only be described as 'absurd' " when applied to the ATA. (Recons. Mem. at 23-24.) This argument, which is unsupported by citation to legal authority, is not properly presented on a motion for reconsideration, and so the court does not address it.

Plaintiffs' claims. (*Id.* at 24-25.) From this, Plaintiffs contend that the court should not have applied Section 230 to the Israeli law claims, as the CDA "is a feature of American law that has no corollary in Israel." (*Id.* at 25.)

Plaintiffs' argument misunderstands the court's prior opinion, which addressed the issue raised. Noting that Plaintiffs contended that Section 230 "does not apply to claims based in foreign law," the court assumed that the Plaintiffs' Israeli tort claims were properly presented and concluded those claims were barred in any event. (May 18 M & O at 27 n.14.) In coming to this determination, the court examined the enumerated exceptions to Section 230's grant of immunity, and concluded that the absence of any carve-out for claims based on foreign law indicated that no such exception was intended. (*Id.*)

To the extent that Plaintiffs argue that a conflict-of-laws analysis prevents the application of federal statutes to foreign-law-based claims, the argument is unsupported in law or logic. Plaintiffs point to no authority for the notion that the decisional rules applied in a conflict-of-laws analysis require courts in this country to ignore governing sources of federal law when applying claims raised under the laws of other nations,[5] nor is the court aware of any such authority.

---

[5] Instead, Plaintiffs cite to cases considering conflicts of law between the laws of individual *states* and other states or foreign nations or between the laws of two foreign nations. *See Licci ex rel. v. Lebanese Canadian Bank, SAL,* 672 F.3d 155, 157-58 (2d Cir. 2012); *Fin. One Pub. Co. Ltd. v. Lehman Bros. Special Fin.,*

Further, Plaintiffs' suggestion appears to be fundamentally at odds with supremacy of federal law over state law. When conducting a conflict-of-laws analysis, federal courts look to the law of the forum state, in this case New York. *Cf., e.g.*, *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL,* 672 F.3d 155, 157 (2d Cir. 2012) ("A federal court sitting in diversity or adjudicating state law claims that are pendent to a federal claim must apply the choice of law rules of the forum state." (internal quotation marks and citation omitted)). It is almost too obvious to state that New York law, including the law governing conflict of laws, could not direct courts to disregard federal law. *Cf. Figueroa v. Foster,* 864 F.3d 222, 227 (2d Cir. 2017) ("Under the Supremacy Clause of the Constitution, state and local laws that conflict with federal law are without effect." (internal quotation marks and citation omitted)). Finally, the court notes that the application of Section 230's affirmative defense to Israeli claims is sensible under the circumstances, as it avoids the perverse result that plaintiffs could bring claims in American courts under foreign law that would be barred if brought under federal or state law.

Inc., 414 F.3d 325, 331-339 (2d Cir. 2005) (same as to New York and Thai law); *Cooney v. Osgood Mach., Inc.,* 81 N.Y.2d 66, 75, 595 N.Y.S.2d 919, 612 N.E.2d 277 (N.Y. 1993) (same as to New York and Missouri law); *Schultz v. Boy Scouts of Am., Inc.,* 65 N.Y.2d 189, 194-204, 491 N.Y.S.2d 90, 480 N.E.2d 679 (N.Y. 1985) (same as to New York and New Jersey law); *Wultz v. Islamic Rep. of Iran,* 755 F.Supp.2d 1, 78-80 (D.D.C. 2010) (same as to laws of China and Israel).

Accordingly, and again assuming that Israeli law, not New York law, applies to the cited claims, the court is not convinced that its prior decision was erroneous.

* * *

For the foregoing reasons, Plaintiffs' motion to alter the judgment pursuant to Federal Rule of Civil Procedure 59(e) is DENIED.

B. Motion to Amend the Complaint

In the alternative, Plaintiffs move to amend their complaint a second time and propose new allegations which, in their account, correct the deficiencies in their prior complaint. (Amendment Mot.; Pls. Mem. in Supp. of Amendment Mot. ("Amendment Mem.") (Dkt. 53); *see also* PSAC.) After considering the proposed second amended complaint, the court concludes that Plaintiffs fail to allege facts that would support any of the asserted causes of action against Facebook. Their motion to amend is accordingly denied.

1. Legal Standard

Under Federal Rule of Civil Procedure 15(a), a party may amend its complaint either with its opponent's written consent or with leave of the court.[6] Fed. R. Civ. P. 15(a)(2). Courts "should freely give leave [to

[6] Rule 15(a) also permits amendment once as a matter of course within set time periods. That provision is not relevant here, however, not least because Plaintiffs have already amended their complaint once before.

amend] when justice so requires." *Id.* Accordingly, requests to amend should be [sic] generally be granted absent a showing of " 'undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . . [or] futility of amendment.' " *Conforti v. Sunbelt Rentals, Inc.,* 201 F.Supp.3d 278, 290-91 (E.D.N.Y. 2016) (quoting *Dougherty v. Town of N. Hempstead Bd. of Zoning Appeals,* 282 F.3d 83, 87 (2d Cir. 2002)) (alterations in original). In considering whether an amendment would be "futile," courts apply the same standard of legal sufficiency as that employed in motions to dismiss, *see Thea v. Kleinhandler*, 807 F.3d 492, 496-97 (2d Cir. 2015), considering whether the proposed amended complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face,' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)).

Leave to amend may be granted post-judgment. "As a procedural matter, '[a] party seeking to file an amended complaint postjudgment must first have the judgment vacated or set aside pursuant to [Rules] 59(e) or 60(b).' " *Williams v. Citigroup Inc.,* 659 F.3d 208, 213 (2d Cir. 2011) (quoting *Ruotolo v. City of New York,* 514 F.3d 184, 191 (2d Cir. 2008)). In such cases, however, "Rule 15's liberality must be tempered by considerations of finality." *Id.*

2. Application

In their proposed second amended complaint ("PSAC"), Plaintiffs propose to add a number of allegations that fall into four primary categories: (1) "[f]actual background and legislative statements involved in the enactment of the federal antiterrorism statutes at issue" (Amendment Mem. at 4); (2) allegations that Facebook violated the ATA by providing material support to Hamas in the form of "personnel" and "expert assistance" (*id.* at 3-4), and that Facebook's assistance to Hamas "freed-up money and other resources for Hamas and the terrorists to carry out the terrorist acts that severely injured the Plaintiffs" (*id.* at 7); (3) allegations related to Facebook users' ability to "self-publish" (*id.* at 4); and (4) Allegations demonstrating that Facebook's actions pertaining to its provision of material support and resources to Hamas occurred" outside of the United States (*id.* at 6). Additionally, Plaintiffs propose adding a new claim under 18 U.S.C. § 2339C(c) based on Facebook's purported concealment of material resources provided to Hamas, as well as factual allegations related to that claim. The court examines each of these categories of proposed amendments and, for the reasons that follow, denies the motion to amend as futile.

a. Allegations Regarding Antiterrorism Statutes

The first category of new proposed new allegations pertains only to the background of the two antiterrorism statutes at issue here, the ATA and JASTA. (*Id.* at

4.) These allegations include a history of the ATA's enactment (PSAC ¶¶ 2-7, 18-53), including specifically the act's civil enforcement provisions (*id.* ¶¶ 38-44). Plaintiffs' evident purpose in introducing this background is to demonstrate that civil claims for material support fall outside of Section 230's grant of immunity based on an exception within that section, which states that "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . Federal criminal statute." 47 U.S.C. § 230(e)(1). Plaintiffs contend that the background and legislative history of the ATA and JASTA show that the creation of civil remedies for violations of criminal statutes prohibiting terrorism were meant to facilitate "enforcement" of those statutes.[7] (Pls. Reply in Supp. of Amendment Mot. ("Amendment Reply") (Dkt. 59) at 2-3.)

Plaintiffs' arguments are unpersuasive. The court addressed Section 230's exception for enforcement of federal criminal laws in its previous opinion, noting that "most courts that have examined" that subsection have concluded that it does not "inhibit immunity as to civil liability predicated on federal criminal statutes."

---

[7] Plaintiffs also argue that the text and legislative history of the ATA and, particularly, JASTA, demonstrate that "Congress deems ATA claims supremely important, and insofar as other statute or regulations—including the CDA—are inconsistent with this most recent expression of Congress's intent, the ATA claims must prevail." (Pls. Reply in Supp. of Amendment Mot. ("Amendment Reply") (Dkt 59) at 4-6.) This argument effectively retreads Plaintiffs' contention that the ATA and JASTA implicitly repeal the CDA to the extent of any conflict. For the same reasons that it denied the motion for reconsideration, the court concludes that Plaintiffs' proposed amendments on this point are futile.

(May 18 M & O at 21 n.11.) In this regard, the court finds particularly convincing the First Circuit's conclusion that Section 230(e)(1)'s specific reference to "criminal statutes," viewed alongside other exceptions within Section 230 that apply equally to civil and criminal remedies, indicates that Congress only intended to exclude criminal prosecutions through that exception.[8] *Jane Doe No. 1 v. Backpage.com*, 817 F.3d 12, 23 (1st Cir. 2016). The court agrees with this reasoning and concludes that the "enforcement"[9] of "Federal criminal

---

[8] Plaintiffs attempt to distinguish *Jane Doe* and other cases cited in the court's previous opinion on the basis that the statutes cited therein "permitted recovery of compensatory damages, *not* punitive or exemplary damages [as] permitted by the ATA." (Amendment Reply at 3 (emphasis in original).) However, the First Circuit reasoned in *Jane Doe* from the language of the statute itself that Section 230(e)(1) excepts only criminal actions to enforce criminal statutes, 817 F.3d at 23, which means that the purposes of a particular civil action are irrelevant. Further, the court notes that Plaintiffs appear to be incorrect in their contention that the statute at issue in *Jane Doe* does not permit punitive damages in civil suits. While the statute and Second Circuit case law do not provide direct guidance on the point, the Ninth Circuit concluded that the civil remedies available under that section include punitive damages. *See Ditullio v. Boehm,* 662 F.3d 1091, 1098 (9th Cir. 2011); *see also Walia v. Veritas Healthcare Solutions, L.L.C.,* No. 13-CV-6935 (KPF), 2015 WL 4743542, at *10 n.15 (S.D.N. Y Aug. 11, 2015).

[9] Plaintiffs point to a statement by the Second Circuit that "the ATA's legislative history reflects that Congress conceived of the ATA, at least in part, as a mechanism for protecting the public's interests through private enforcement." *Linde v. Arab Bank, PLC,* 706 F.3d 92, 112 (2d Cir. 2013). The court is not convinced that this language, which appears in dicta and arose in the entirely different context of international comity analysis, implies that private suits to enforce the ATA are, in effect, on the same footing as are prosecutions under that law. Moreover, as stressed

statutes" in this context was intended only to extend to enforcement *by means of a criminal proceeding*.

Accordingly, the court finds these new allegations regarding the history and purpose of the ATA and JASTA to be insufficient to overcome previously identified shortcomings in Plaintiffs' first amended complaint.

b. Additional Material Support Allegations and Self-Publication

Plaintiffs' proposed complaint also attempts to refine its allegations that Facebook provided material support to terrorism so as to avoid involving implicating Facebook's role as a publisher or speaker of third-party content. First, Plaintiffs attempt to differentiate Facebook from other websites by stressing that Facebook users register to "design and create their own internet website," from which they are free to "self-publish" content without Facebook purporting to act as "editor, publisher, or speaker" of its users' postings. (PSAC ¶ 127-28.) Second, Plaintiffs add new allegations regarding the types of "material support" that Facebook provides. They characterize Facebook as providing "personnel" to Hamas by "making Hamas leaders,

---

above, the task before the court is not to interpret the ATA, but to determine the meaning of Section 230(e)(1). As the court has already determined that Section 230's reference to "enforcement . . . of any . . . Federal criminal statutes" is specific to criminal prosecutions, it need not ascertain whether civil provisions of other statutes were envisioned as providing a secondary means of enforcement.

operatives, and recruits available to Hamas to conspire, plan, prepare, and carry out terrorist activity." (PSAC ¶ 223.) Plaintiffs also contend that Facebook provides "expert services" to Hamas-affiliated users by allowing them access to its platform and, through such access, "highly advanced software, algorithms, computer servers and storage, communications devices, [and] computer applications" that Facebook provides to all users. (*Id.* ¶¶ 123-24; *see also* Amendment Mem. at 5.)

Plaintiffs' additional allegations do nothing to address the shortcomings in their theories of liability identified in the court's previous decision. With respect to the allegations regarding "self-publication," Plaintiffs misinterpret the scope of Section 230's immunity. Plaintiffs repeatedly stress that users' introduction of information onto Facebook's eponymous platform occurs without Facebook "exercis[ing] any editorial discretion when providing registered accounts or over what users publish on their own [] accounts." (Amendment Reply at 8.) From this, Plaintiffs appear to suggest that Facebook cannot be exercising any editorial or publication functions protected by Section 230 which, they imply, require some specific selection with respect to the particular users or postings that may appear on its platform. This argument misunderstands the court's prior decision: In the court's view, Facebook's decision to keep its platform as an open forum, available for registration and posting without prior approval from Facebook, is itself an exercise of editorial

discretion. (May 18 M & O at 21.) As noted by the First Circuit:

> [the plaintiffs-appellants'] well-pleaded claims address the structure and operation of the [defendant-appellee's] website, that is, [defendant's] decisions about how to treat postings. Those claims challenge features that are part and parcel of the overall design and operation of the website (such as the lack of phone number verification, the rules about whether a person may post after attempting to enter a forbidden term, and the procedure for uploading photographs). Features such as these, which reflect choices about what content can appear on the website and in what form, are editorial choices that fall within the purview of traditional publisher functions.

Jane Doe, 817 F.3d at 21. The same reasoning supports both the court's previous decision and its conclusion here that allegations regarding "self-publication" do not exempt Plaintiffs' claims from Section 230's coverage: Facebook's decisions regarding the "overall design and operation of its website," including the criteria (or lack thereof) for obtaining an account and posting on the platform are themselves "editorial choices that fall within the purview of traditional publisher functions." *Id.*; *see also Fields v. Twitter, Inc.*, 217 F.Supp.3d 1116, 1124 (N.D. Cal. 2016) (holding that the defendant's "decisions to structure and operate itself as a 'platform . . . allow[ing] for the freedom of expression of hundreds [of] millions of people around the world,' and, through its hands-off policy, allowing [a terrorist group] to

obtain 'dozens of accounts on its social network' 'reflect choices about what [third-party] content can appear on [Twitter] and in what form.'" (internal quotation marks and citations omitted; alterations in original)). Plaintiffs' new allegations that these policies allow users to join Facebook's platform and to "self-publish" without Facebook's prior approval do not alter the conclusion that Facebook's decisions regarding the structure of its platform fall within the traditional functions of a publisher and so that Plaintiffs' theory relies only on a "duty . . . derive[d] from [Facebook's] status or conduct as a 'publisher or speaker.'" *LeadClick Media,* 838 F.3d at 175.

Plaintiffs' new allegations regarding Facebook's alleged provision of "personnel" and "expert services" to Hamas and Hamas-affiliated users suffer from the same flaw. Plaintiffs claim that "technological tools" Facebook provided to its users, and that these tools are unrelated to the content of the underlying communications. (Amendment Reply at 8; *see also* Amendment Mem. at 4-5.) Plaintiffs contend these tools provided to users "extend[] far beyond providing or performing traditional services of a publisher," and so are not within the scope of the services of a 'publisher.'" (Amendment Reply at 7-8.) At root, however, these theories again derive from a claimed duty on Facebook's part to prevent certain users from using its platform and seek to impose liability based on Facebook's decision to allow free access to, and use of, its platform and forum. Said differently, Facebook is alleged to have violated a duty to prevent certain users from accessing

and using its platform. As discussed above and in this court's previous dismissal of Plaintiffs' claims, Section 230 shields Facebook from such claims, as "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally 'derive[] from [Facebook's] status or conduct as a 'publisher or speaker.'" (May 18 M & O at 21 (quoting *LeadClick Media*, 838 F.3d at 175).)

Moreover, like Plaintiffs' first amended complaint, Plaintiffs' new allegations regarding Facebook's claimed provision of "personnel" and "expert services" again "rely on content to establish causation and, by extension, Facebook's liability," a theory already rejected by this court. (May 18 M & O at 22.) As Plaintiffs' proposed amended complaint makes clear, their theory that Facebook makes "personnel" available to Hamas depends on the content of communications on Facebook's website: Plaintiffs seek to hold Facebook liable for providing a publication forum for Hamas and its leaders, operatives, and recruits, "to conspire, plan, prepare, and carry out terrorist activity." (SAC ¶ 223.) This is fundamentally no different than Plaintiffs' prior argument that "Facebook contributed to their harm by allowing Hamas to use its platform to post particular offensive content." (May 18 M & O at 22.) Likewise, both the "personnel" and "expert services" allegations appear to rest in large part on allegations that Facebook's networking algorithms recommend content to account holders. However, as Facebook points out, "the

features of Facebook that [P]laintiffs criticize operate *solely* in conjunction with . . . content posted by Facebook users." (*See* Def. Opp'n to Amendment Mot. ("Amendment Opp'n") (Dkt. 57) at 5 (emphasis in original)); *see also* PSAC ¶¶ 611-22 (describing how Facebook's algorithms connect "users to one another and to groups and events that they will be interested in based on the information in their user profiles and online activities"). Plaintiffs' new allegations would again simply seek to hold Facebook liable solely on the basis of the website's role in hosting and re-publishing content generated by Hamas-affiliated users.[10] Bound up as they are in the content that Hamas-affiliated users provide, the court concludes that these new claims remain subject to the immunity afforded under Section

[10] Plaintiff also proposes to add new allegations regarding additional "predicate" acts of terrorism by Hamas. (PSAC ¶¶ 648-49; Amendment Mem. at 7.) Plaintiffs contend that these additional predicate acts support the conclusion that "Facebook's liability does *not* depend upon attributing the content of Hamas' Facebook posts to Facebook." (Amendment Mem. at 7.) In particular, Plaintiffs point to the "aiding and abetting" charges brought under JASTA and argue that "once Facebook . . . provid[es] material support to Hamas, Facebook is liable under [JASTA] for any reasonably foreseeable injury that may result from Hamas's use of that material support." (Amendment Reply at 9.) These proposed amendments do nothing to address or sidestep the basis for the court's prior dismissal of Plaintiffs' claims: regardless of the predicate acts at issue, the only basis that Plaintiffs propose for imposing liability on Facebook for "aiding and abetting" or providing "material support" to those terroristic crimes is Facebook's decision to permit Hamas-affiliated users to use its platform. The court has repeatedly rejected that theory, and so the proposed amendments do not further Plaintiffs' entitlement to relief.

230 and so cannot provide a basis for liability as to Facebook.[11]

c. Extraterritoriality Allegations

Plaintiffs' proposed amendments include a number of factual allegations regarding Facebook's conduct outside of the United States, which Plaintiffs contend "support [their] contention that the CDA does not apply to claims involving violation of laws outside of the territorial jurisdiction of the United States." (Amendment Reply at 10; PSAC ¶¶ 629-32.) The court need not dwell on these new allegations. The court concluded in its prior opinion that, for purposes of the extraterritoriality analysis, the relevant territorial relationships are based "where redress is sought and immunity is needed"—the situs of the litigation. (May 18 M & O at 27.) Plaintiffs' new allegations obviously do not suggest that the situs of this litigation has changed, but are better viewed as part of their tenacious effort to convince the court to reconsider its prior extraterritoriality analysis. The court has already declined to do

[11] Plaintiffs also propose alleging that, because of its use of Facebook, Hamas was able to "allocate other financial resources to terrorist activities." (Amendment Reply at 10; *see also* PSAC ¶ 219.) Plaintiffs are correct that this allegation could support a claim under the material support statutes. *See, e.g.*, *Holder v. Humanitarian Law Project,* 561 U.S. 1, 30, 130 S.Ct. 2705, 177 L.Ed.2d 355 (2010). In light of the court's conclusion that the Plaintiffs' material support claims are not viable because they rely on theories barred by Section 230, however, these allegations do not support Facebook's liability.

so, and so concludes that these new allegations fail to advance Plaintiffs' claims.

d. "Concealment" of Material Support

Plaintiffs' final set of new allegations relates to their new claim that Facebook "concealed" its provision of material support to Hamas in violation of the ATA. Specifically, Plaintiffs allege that Facebook's "Community Standards," which purport to prevent terrorists and terrorist organizations to use the platform, "conceal" both Facebook's own provision of material support to Hamas and the separate use of the platform by terrorists to provide material support to Hamas. (Amendment Mem. at 6.)

The relevant section of the material support statutes prohibits covered individuals and entities[12] from "knowingly conceal[ing] or disguis[ing] the nature, location, source, ownership, or control of any material support or resources, or any proceeds of such funds . . . knowing or intending that the support or resources are to be provided, or . . . were provided, in violation of section 2339B[.]" 18 U.S.C. § 2339C(c)(2)(A). Thus, in order to violate that provision, the entity must have knowingly "concealed" or "disguised" material support

[12] Specifically, the prohibition applies to individuals and entities in the United States or outside of the United States if they are either "a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possession)[.]" 18 U.S.C. § 2339C(c)(1)(A)-(B). Facebook does not argue that it falls outside this coverage.

provided to a designated foreign terrorist organization[13] but need not necessarily have provided the material support itself.

In the court's view, allegations brought under that section against Facebook, if plausibly pled, would escape Section 230's coverage. In its opposition to the amendment, Facebook argues strenuously that the "concealment claim boils down to a challenge to who may use Facebook and what content they share" and so seeks to impose liability on the same basis already rejected by the court. (Def. Suppl. Opp'n to Amendment Mot. (Dkt. 60) at 3.) It may be true that a concealment claim based only on Facebook's own purported provision of material support would fail: As noted, Section 2339C(c) requires a predicate violation of Section 2339B, 18 U.S.C. § 2339C(c)(2)(A), and the court has already held that Facebook cannot be held liable under that statute based on Plaintiffs' theories. Plaintiffs also contend, however, that Facebook's statements in the Community Standards "conceal" acts by Hamas members and supporters that provide material support to Hamas using Facebook's platform. (Amendment Mem., at 6 ("By its actions and deceptions, Facebook also conceals the Hamas leaders' and affiliates' *own* provision of personnel (themselves) via their Facebook accounts." (emphasis in original)); PSAC ¶¶ 222-24.) Said differently, unlike the other theories of liability proposed by Plaintiffs, the "concealment"

[13] 18 U.S.C. § 2339B applies only to material support provided to designated foreign terrorist organizations. 18 U.S.C. § 2339B(a).

claim does not seek to hold Facebook liable for failing to prevent Hamas and its affiliates from obtaining accounts or posting offensive content. (*See* May 18 M & O, at 21-22.) Instead, Plaintiffs argue that Facebook's own actions conceal or disguise material support to Hamas provided by others. The court agrees that, thus construed, the concealment cause of action does not fall within the coverage of Section 230, as it does not "inherently require[ ] the court to treat [Facebook] as the publisher or speaker of content provided by another," or "derive[ ] from [Facebook's] status or conduct as a 'publisher or speaker.'" (*Id.* at 20 (quoting *LeadClick Media,* 838 F.3d at 175)).

This does not end the inquiry, however, as Plaintiffs must still set forth sufficient allegations "to state a claim to relief that is plausible on its face." *Iqbal,* 556 U.S. at 678, 129 S.Ct. 1937 (internal quotation marks and citation omitted). The key question in this instance is whether the proposed amendments set forth a sufficient factual basis for the court to conclude that Facebook "concealed" or "disguised" material support to Hamas provided using its platform. The statute does not define those terms, nor does any court appear to have interpreted them in the context of this or similar statutes.[14] "[W]here a statute does not define a term,

[14] Similar language appears in 18 U.S.C. § 2339A (criminalizing "conceal[ing] or disguis[ing] the nature, location, source, or ownership of material support or resources") and various places in 18 U.S.C § 1956 (defining money laundering transaction to include transactions intended "to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity"). The court reviewed cases

we give the term its ordinary meaning." *EMI Christian Music Grp., Inc. v. MP3Tunes, LLC,* 844 F.3d 79, 89 (2d Cir. 2016) (internal quotation marks and citation omitted). The Merriam-Webster dictionary defines "conceal" as, *inter alia,* "to prevent disclosure or recognition of," *Conceal,* Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/conceal (last visited Jan. 8, 2018), and "disguise" as, *inter alia,* "to obscure the existence or true state or character of," *Disguise*, Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/disguise (last visited Jan. 8, 2018). Thus, in order to avoid the conclusion that leave to amend should be denied as futile, Plaintiffs must present facts sufficient to show that Facebook's actions either prevented "disclosure or recognition" of Hamas' use of its platform or "obscured the existence or true state or character" of that use.

After examining the allegations set forth in the proposed amended complaint, the court concludes that Plaintiffs fail to set forth a plausible claim that Facebook "concealed" or "disguised" the use of its platform by Hamas and its member [sic] and supporters. As noted, Plaintiffs' claims that Facebook conceals Hamas's presence on its platform are based solely on allegedly false claims in Facebook's "Community Standards" and public statements by the company that it does not permit terrorists or terrorist organizations to use the website. (*See* Pls. Suppl. Mem. in Supp. of Amendment Mot. (Dkt. 61) at 5-6; *see also, e.g.,* PSAC ¶¶ 172-74, 583-89.)

---

interpreting the terms "conceal" and "disguise" in the context of those statutes as well, but found no helpful guidance.

Plaintiffs do not allege, however, that such false statements had the effect of preventing anyone from discovering that Hamas or its members were using Facebook's platform. At most, the policy statements and public pronouncements to which Plaintiffs point have the effect of concealing or disguising Facebook's factual willingness to abide such use, but not the fact of the use itself. To the contrary, the complaint is replete with allegations that "HAMAS, its leaders, spokesmen, and members have openly maintained and used official Facebook accounts" (PSAC ¶ 9), use those accounts to draw attention to their activities (PSAC ¶ 165), and that this use of the platform by Hamas and other, similar groups has been widely recognized by the public (*id.* ¶¶ 590-98). Against these allegations, the court sees no plausible claim that Facebook's statements—or any other action by the company, for that matter—did anything to "prevent disclosure or recognition" or "obscure the existence or true . . . character of" the use of its platform to support Hamas.[15]

---

[15] In their supplemental brief in support of the concealment claim, Plaintiffs also request leave to amend their complaint—again—to include allegations related to testimony by Facebook's general counsel before the United States Senate. (Pls. Suppl. Mem. in Supp. of Amendment Mot. at 9-10.) Plaintiffs do not, however, state how this information would support any of their claims, leaving the court without any basis to assess the utility or futility of such amendments. Particularly in light of court's existing judgment against Plaintiff, the court finds that considerations of finality outweigh any interest in allowing Plaintiffs to submit another round of amendments and denies the motion accordingly. *Cf. Williams,* 659 F.3d at 213 ("Where . . . a 'party does not seek leave to file an amended complaint until after judgment is

* * *

Accordingly, Plaintiffs' motion to amend their complaint is pursuant to Federal Rules of Civil Procedure 15(a), 59(e), and 60(b) is denied. Moreover, as the proposed amendments fail to correct the deficiencies identified by the court's decision dismissing Plaintiffs' first amended complaint, the court concludes that it is appropriate to deny the motion with prejudice. *See, e.g., Curtis v. Citibank, N.A.,* 204 Fed.Appx. 929, 932 (2d Cir. 2006) (summary order) (holding that dismissal with prejudice was within the court's discretion where plaintiff had notice of and failed to correct deficiencies in complaint).

III. CONCLUSION

For the foregoing reasons, Plaintiffs' motions to amend the judgment (Dkt. 50) and to file a second amended complaint (Dkt. 52) are DENIED WITH PREJUDICE.

SO ORDERED.

---

entered, Rule 15's liberality must be tempered by considerations of finality.' ").

252 F.Supp.3d 140
United States District Court, E.D. New York.

Racheli COHEN, et al., Plaintiffs,
v.
FACEBOOK, INC., Defendant.
Stuart Force, Individually and as Administrator on Behalf of the Estate of Taylor Force, et al., Plaintiffs,
v.
Facebook, Inc., Defendant.

16–CV–4453 (NGG) (LB)
|
16–CV–5158 (NGG) (LB)
|
Signed 05/18/2017

Attorneys and Law Firms

Robert Joseph Tolchin, The Berkman Law Office, LLC, Brooklyn, NY, for Plaintiff.

Craig S. Primis, Jennifer M. Bandy, Kenneth W. Allen, Kirkland & Ellis LLP, Washington, DC, Paul S. Grewal, Facebook, Inc., Menlo Park, CA, Shireen Anneke Barday, Thomas Aulden Burcher-DuPont, Kirkland & Ellis LLP, New York, NY, for Defendant.

MEMORANDUM & ORDER

NICHOLAS G. GARAUFIS, United States District Judge.

Plaintiffs in the above-captioned related actions assert various claims against Facebook, Inc. ("Facebook") based on their contention that Facebook has

supported terrorist organizations by allowing those groups and their members to use its social media platform to further their aims. The plaintiffs in the first action (the "Cohen Action") are roughly 20,000 Israeli citizens (the "Cohen Plaintiffs"). (Cohen Am. Compl. ("Cohen FAC") (Dkt. 17), No. 16–CV–4453.) The second action (the "Force Action") is brought by victims, estates, and family members of victims of terrorist attacks in Israel (the "Force Plaintiffs" and, together with the Cohen Plaintiffs, "Plaintiffs"). (Force Am. Compl. ("Force FAC") (Dkt. 28), No. 16–CV–5158.)

Before the court are Facebook's motions to dismiss the operative complaints in both actions pursuant to Federal Rules of Civil Procedure 12(b)(1), (2), and (6) (as to the Cohen Action) and 12(b)(2) and (6) (as to the Force Action). (Cohen Def. Mot. to Dismiss ("Cohen MTD") (Dkt. 23), No. 16–CV–4453; Force Def. Mot. to Dismiss ("Force MTD") (Dkt. 34), No. 16–CV–5158.) Because of the substantial similarity in facts and the legal issues raised, the court addresses these motions together in this Memorandum and Order.

For the following reasons, the court GRANTS Facebook's motions to dismiss the operative complaints in both the Cohen Action and the Force Action.

I. BACKGROUND

A. Facebook's Social Media Platform

Facebook's eponymous social media website allows users to create personalized webpages that contain

information about themselves, including identifying information, photographs, videos, interests, recent activities, and links to content from other websites. (Cohen FAC ¶ 42; *see also* Force FAC ¶¶ 94–95, 522.) Once a user joins the website, they can engage with other Facebook users in a number of ways, including by adding those users as "friends" and providing feedback to content provided by other users by "sharing," "liking" (i.e. applying a tag that is shared with other users), or commenting on that content. (Cohen FAC ¶ 42; Force FAC ¶ 523.) Additionally, users are able to view their contacts' activities on the website, including both information posted by those contacts as well as their contacts' interactions with other users and content. (*See* Cohen FAC ¶ 42; Force FAC ¶¶ 524, 527.)

Facebook users are also able to create "groups" with other users, which allows multiple users to join a shared website which has its own profile and information. (Cohen FAC ¶ 43; Force FAC ¶ 525–26.) Members of a group can view, interact with, and share content posted in these group forums. (Cohen FAC ¶ 43.)

Facebook collects data as to its users' activities through the website, including but not limited to information regarding contacts and group associations, content that users post and interact with, and use of third party websites. (Cohen FAC ¶ 44; Force Compl ¶ 528.) Using proprietary algorithms, Facebook generates targeted recommendations for each user, promoting content, websites, advertisements, users, groups, and events that may appeal to a user based on their

usage history. (Cohen FAC ¶¶ 45–48; Force FAC ¶¶ 529–41.) In this way, Facebook connects users with other individuals and groups based on projected common interests, activities, contacts, and patterns of usage. (Cohen FAC ¶ 48; Force FAC ¶¶ 530–33.) Facebook also presents users with content posted by other users, groups, and third parties (e.g., advertisers) that is likely to be of interest to them, again based on prior usage history. (Cohen FAC ¶¶ 53–55; Force FAC ¶¶ 534–41.)

B. The Plaintiffs

The Cohen Plaintiffs are 20,000 individuals residing in Israel who state that they "have been and continue to be targeted by" attacks by Palestinian terrorist organizations. (Cohen FAC ¶ 4.) The Cohen Plaintiffs claim that they are "presently threatened with imminent violent attacks that are planned, coordinated, directed, and/or incited by terrorist users of Facebook." (*Id.* ¶ 5.) In particular, they claim to be threatened by an outbreak of violence by Palestinian groups—which they sometimes refer to as the "Facebook Intifada"—and their Complaint recounts 54 separate attacks by Palestinian terrorists and terror groups in Israel since October 1, 2015. (*Id.* ¶¶ 11–16.)

Unlike the Cohen Plaintiffs, who claim to be threatened only by potential future attacks, the Force Plaintiffs are the estates of victims (and, in one case, the surviving victim) of past attacks by the Palestinian terrorist organization Hamas and the family members

of those victims. (Force FAC ¶¶ 5–18). The victims were U.S. citizens, most of whom were domiciled in Israel at the time of the attacks. (*See id.*) In their Complaint, the Force Plaintiffs describe the attacks that harmed them, providing a detailed timeline of the events and Hamas's particular involvement in the attacks. (*See generally id.* ¶¶ 156–499.)

C. Allegations Against Facebook

Plaintiffs in the two actions make substantially similar allegations as to Facebook's role in their alleged harms. Plaintiffs claim that Palestinian terrorists[1] "use Facebook's social media platform and Communications services to incite, enlist, organize, and dispatch would-be killers to 'slaughter Jews.'" (Cohen FAC ¶ 18; *see also* Force FAC ¶ 362.) They further aver that Palestinian terrorist groups and associated individuals use their Facebook pages for general and specific incitements to violence and to praise past terrorist attacks. (*See* Cohen Compl ¶¶ 23–36; Force FAC ¶¶ 111–15.) Plaintiffs allege that Facebook's algorithms, used to connect users with other users, groups, and content that may be of interest to them, play a vital role in spreading this content, as Palestinian terrorist organizations are able to "more effectively disseminate [incitements to violence], including commands to murder Israelis and Jews, to those most

[1] While the Cohen Complaint refers to Palestinian terrorists and terrorist groups generally, the allegations in the Force Complaint are specific to Hamas, and references to both Complaints together should be read accordingly.

susceptible to that message, and who most desire to act on that incitement." (Cohen FAC ¶ 56; *see also* Force FAC ¶¶ 530–41.)

Plaintiffs allege that Facebook is aware of the use of its platform by Palestinian terrorist organizations and their members but has failed to take action to deactivate their accounts or prevent them from inciting violence. (Cohen FAC ¶ 40; Force FAC ¶ 502–04.) In the case of Hamas, the Force Complaint alleges that Facebook allows that organization, its members, and affiliated organizations to operate Facebook accounts in their own names, despite knowledge that many of them have been officially named as terrorists and sanctioned by various governments. (*See* Force FAC ¶¶ 118–25.) Plaintiffs claim that Facebook's approach to addressing this use of the platform has been piecemeal (intermittently deleting individual postings or banning users) and inconsistent (e.g., deleting offending posts from one individual without removing identical messages or banning users without taking steps to ensure that the same person does not subsequently rejoin the website under a different moniker). (*Id.* ¶¶ 549–55; *see also* Cohen FAC ¶¶ 40, 61–62.)

II. PROCEDURAL HISTORY

The Cohen Plaintiffs originally filed their action in the Supreme Court of New York, Kings County, and it was removed to this court by Facebook on August 10, 2016, on the basis of diversity of citizenship. (Not. of Removal (Dkt. 1), No. 16–CV–4453.) The operative

complaint in this action is the First Amended Complaint, filed on October 10, 2016. (*See generally* Cohen FAC.) The Cohen Plaintiffs bring Israeli law claims of negligence, breach of statutory duty, and vicarious liability (*id.* ¶¶ 67–106), as well as New York law claims for prima facie tort, intentional infliction of emotional distress, aiding and abetting a tort, and civil conspiracy (*id.* ¶¶ 107–34). The Cohen Plaintiffs seek only declaratory and injunctive relief. (*Id.* ¶¶ 149–55.) Separate from their substantive claims for relief, the Cohen Complaint requests a judicial declaration that the causes of action noted above are not barred by Section 230(c)(1) of the Communications Decency Act, 47 U.S.C. § 230. (*Id.* ¶¶ 135–48)

The Force Plaintiffs filed their action in the United States District Court for the Southern District of New York on July 10, 2016. (*See generally* Force Compl. (Dkt. 1), No. 16–CV–5158.) The case was subsequently transferred to this court as related to the Cohen Action on September 16, 2016. (Sept. 16, 2016, Order Reassigning Case (Dkt. 15).) The operative complaint is the First Amended Complaint, filed on October 10, 2016. (Force FAC.) Like the Cohen Complaint, the Force Complaint brings claims for negligence, breach of statutory duty, and vicarious liability under Israeli law. (*Id.* ¶¶ 586–620.) The Force Complaint also raises claims under the civil enforcement provisions of the federal Anti-Terrorism Act ("ATA") and the Justice Against Sponsors of Terror Act for aiding and abetting acts of international terrorism, conspiracy in furtherance of acts of international terrorism, and providing

material support to terrorist groups in violation of 18 U.S.C. §§ 2339A and 2339B. (*Id.* ¶¶ 561–85.) The Force Plaintiffs seek $1 billion in compensatory damages, punitive damages to be determined at trial, and treble damages for violations of the federal anti-terrorism statutes. (*Id.* at ECF p.123.)

III. DISCUSSION

Before the court are Facebook's motions to dismiss the operative complaints in each of the two actions. (Cohen MTD; Force MTD.) Facebook moves to dismiss the Cohen Complaint for lack of subject matter and personal jurisdiction and for failure to state a claim upon which relief may be granted pursuant to Rules 12(b)(1), (2), and (6) of the Federal Rules of Civil Procedure. (Cohen MTD; *see also* Mem. in Supp. of Def. Mot. to Dismiss ("MTD Mem.") (Dkt. 24), No. 16–CV–4453.)[2] Facebook separately moves to dismiss the Force Complaint for lack of personal jurisdiction and failure to state a claim upon which relief may be granted pursuant to Rules 12(b)(2) and (6). (Force MTD; *see also* MTD Mem.)

A court facing challenges as to both its jurisdiction over a party and the sufficiency of any claims raised

[2] The parties briefed the motions to dismiss together, and their filings in support of and opposition to Facebook's motions to dismiss appear in identical form on both the Cohen and Force dockets. In order to avoid confusion, the court's citations to Facebook's Memorandum in Support of the Motions to Dismiss, Plaintiffs' Response in Opposition to the Motions to Dismiss, and Facebook's Reply are to the entries on the Cohen docket.

must first address the jurisdictional question. *See Arrowsmith v. United Press Int'l*, 320 F.2d 219, 221 (2d Cir. 1963). However, there is no such required ordering as between questions of personal and subject matter jurisdiction. *Ruhrgas AG v. Marathon Oil Co.*, 526 U.S. 574, 586–87, 119 S.Ct. 1563, 143 L.Ed.2d 760 (1999); *Carver v. Nassau Cty. Interim Fin. Auth.*, 730 F.3d 150, 156 (2d Cir. 2013) (holding that courts "are not bound to decide any particular jurisdictional question before any other").

The court concludes that the Cohen Plaintiffs lack standing to bring their claims and so dismisses their Complaint in its entirety for lack of subject matter jurisdiction. The court finds that it has personal jurisdiction over Facebook with respect to the claims in the Force Complaint but that the action must be dismissed for failure to state a claim, as Facebook makes out a sufficient affirmative defense pursuant to Section 230(c)(1) of the Communications Decency Act.

A. Subject Matter Jurisdiction

Facebook first argues that the Cohen Plaintiffs lack standing to bring their challenges in federal court, as they fail to point to an injury which is either distinguishable from the harm faced by the public at large, fairly traceable to Facebook's actions, or redressable through relief against the company. (*See* MTD Mem. at 30–32.) The court does not address the potential traceability or redressability issues, as it concludes that the

Cohen Plaintiffs do not allege a cognizable "injury-in-fact" and so fail to establish standing.

1. Legal Standard

"A case is properly dismissed for lack of subject matter jurisdiction . . . when the district court lacks the statutory or constitutional power to adjudicate it." *Makarova v. United States,* 201 F.3d 110, 113 (2d Cir. 2000). "The plaintiff bears the burden of alleging facts that affirmatively and plausibly suggest that it has standing to sue," *Cortlandt St. Recovery Corp. v. Hellas Telecomms. S.a.r.l.*, 790 F.3d 411, 417 (2d Cir. 2015) (internal quotation marks, alterations, and citation omitted), a burden which it must satisfy by a preponderance of the evidence, *Luckett v. Bure,* 290 F.3d 493, 496–97 (2d Cir. 2002). Courts must "accept as true all material factual allegations in the complaint. . . . [but] jurisdiction must be shown affirmatively, and that showing is not made by drawing from the pleadings inferences favorable to the party asserting it." *Shipping Fin. Servs. Corp. v. Drakos*, 140 F.3d 129, 131 (2d Cir. 1998); *accord Morrison v. Nat'l Austl. Bank Ltd.*, 547 F.3d 167, 170 (2d Cir. 2008), *aff'd*, 561 U.S. 247, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010).

Federal jurisdiction is constitutionally constrained to "cases" and "controversies," one element of which requires plaintiffs before the court to establish standing: a "genuinely personal stake" in the outcome of a case sufficient to "ensure[ ] the presence of 'that concrete adverseness which sharpens the presentation of issues

upon which [a] court so largely depends.'" *Cortland St. Recovery*, 790 F.3d at 417 (quoting *Baker v. Carr*, 369 U.S. 186, 204, 82 S.Ct. 691, 7 L.Ed.2d 663 (1962)). "In its constitutional dimension, standing imports justiciability," *Warth v. Seldin*, 422 U.S. 490, 498, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975), and objections to standing are properly made under Rule 12(b)(1), as they are directed at the court's ability to adjudicate an issue as to parties before it, *see, e.g.*, *Tasini v. N.Y. Times Co.*, 184 F.Supp.2d 350, 354–55 (S.D.N.Y. 2002).

2. Standing

In order to meet the "irreducible constitutional minimum" of standing, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, ___ U.S. ___, 136 S.Ct. 1540, 1547, 194 L.Ed.2d 635 (2016) (internal quotation marks and citations omitted). "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 1548 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)). Additionally, Plaintiffs must demonstrate a "present case or controversy" with respect to claims seeking prospective, injunctive relief, *City of L.A. v. Lyons*, 461 U.S. 95, 102–03, 103 S.Ct. 1660, 75 L.Ed.2d 675 (1983), and "past injuries cannot satisfy the injury-in-fact requirement" for such claims,

Vaccariello v. XM Satellite Radio, Inc., 295 F.R.D. 62, 72 (S.D.N.Y. 2013) (citing *Shain v. Ellison*, 356 F.3d 211, 215 (2d Cir. 2004)).

Plaintiffs may, under some circumstances, rely on the risk of a future harm to support their injury in fact, *see Deshawn E. v. Safir*, 156 F.3d 340, 344 (2d Cir. 1998); however, such injuries are only "actual or imminent" where "the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."[3] *Susan B. Anthony List v. Driehaus*, ___ U.S.

---

[3] The Supreme Court's decision in *Clapper v. Amnesty International USA* emphasized that the "[t]hreatened injury must be 'certainly impending' 'to constitute injury in fact' and 'allegations of possible future injury' are not sufficient. 568 U.S. 398, 133 S.Ct. 1138, 1141, 185 L.Ed.2d 264 (2013). While the *Clapper* decision acknowledges certain instances in which the Court previously endorsed standing based on a "substantial risk" that the harm would occur if that underlying risk "may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," *id.* at 1151 n.5, it appeared to treat those cases as an exception to the general rule. However, the Court's subsequent decision in *Susan B. Anthony List v. Driehaus* incorporated the "substantial risk" language into its recitation of the standard for measuring injury in fact. ___ U.S. ___, 134 S.Ct. 2334, 2341, 189 L.Ed.2d 246 (2014). At this point, it is not clear when one or the other standard should be applied, *see Hedges v. Obama*, 724 F.3d 170, 196 (2d Cir. 2013), or even whether those standards are distinct, *see N.Y. Bankers Ass'n Inc. v. City of N.Y.*, No. 13-CV-7212 (KPF), 2014 WL 4435427, at *9 (S.D.N.Y. Sept. 9, 2014). While some courts have applied the potentially lower "substantial risk" analysis in assessing pre-enforcement challenges to laws, such as that considered in *Susan B. Anthony List*, the governing standard for actuality or imminence with regard to other types of claims is less clear. *See. e.g., Hedges,* 724 F.3d at 195–96; *Knife Rights, Inc. v. Vance*, 802 F.3d 377, 384 (2d Cir. 2015). The court need not wade into these questions in the present case. The Cohen Complaint

___, 134 S.Ct. 2334, 2341, 189 L.Ed.2d 246 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S.Ct. 1138, 1147, 185 L.Ed.2d 264 (2013)). A plaintiff alleging only an "objectively reasonable possibility" that it will sustain the cited harm at some future time does not satisfy this requirement. *Clapper*, 133 S.Ct. at 1147–48. For this reason, courts are generally hostile to "standing theories that require guesswork as to how independent decisionmakers will exercise their judgment," *id.* at 1150, which almost by definition require speculation as to the likelihood of injury resulting from the third party's actions.

Moreover, plaintiffs cannot evade the required showing of an "actual or imminent" injury by alleging present harms incurred as a result of their "fear[] of a hypothetical future harm that is not certainly impending," as doing so would allow parties to "repackage" their conjectural injury to "manufacture standing." *Id.* at 1151. Instead, the focus of the standing inquiry remains whether "the threat creating the fear is sufficiently imminent." *Hedges v. Obama*, 724 F.3d 170, 195 (2d Cir. 2013); *see also Lyons*, 461 U.S. at 107 n.8, 103 S.Ct. 1660 ("It is the *reality* of the threat . . . that is relevant to the standing inquiry, not the plaintiff's subjective apprehensions.").

Courts have broadly rejected claims based on the risk of falling victim to a future terrorist attack,

---

relies wholly on possible future injuries untethered from any allegation as to the likelihood or imminence of their occurrence that are insufficient under either standard.

concluding that such harms are impermissibly speculative and so insufficient to confer standing. *See, e.g.*, *Tomsha v. Gen. Servs. Admin.*, No. 15-CV-7326 (AJN), 2016 WL 3538380, at *2–3 (S.D.N.Y. June 21, 2016); *Bernstein v. Kerry*, 962 F.Supp.2d 122, 127–28 (D.D.C. 2013); *People of Colo. ex rel. Suthers v. Gonzales*, 558 F.Supp.2d 1158, 1162 (D. Colo. 2007); *cf. George v. Islamic Rep. of Iran*, 63 Fed.Appx. 917, 918 (7th Cir. 2003) (holding that plaintiffs were "no more likely than the average [] citizen to be victims of future attacks" and so their claimed injury was "purely speculative").

3. Application to the Cohen Complaint

The Cohen Plaintiffs fail to carry their burden of showing that their claims are grounded in some non-speculative future harm. Despite offering extensive descriptions of previous attacks (*see* Cohen FAC ¶¶ 11–16), the Cohen Plaintiffs do not seek redress for past actions but instead seek prospective, injunctive relief based on their allegation that Facebook's actions increase their risk of harm from future terrorist attacks (*see, e.g.*, *id.* ¶¶ 5, 37). This claimed harm relies on multiple conjectural leaps, most significantly its central assumption that the Cohen Plaintiffs will be among the victims of an as-yet unknown terrorist attack by independent actors not before the court. The Cohen Complaint contains no factual allegation that could form a basis to conclude that those individuals *in particular* are at any "substantial" or "certainly impending" risk of future harm. *Susan B. Anthony List*, 134 S.Ct. at 2341. At most, the Complaint shows a

general risk of harm to residents of Israel and impliedly asks the court to extract a risk of harm to the Cohen Plaintiffs based on this risk. Without further allegations, however, the court sees no basis to conclude that the Cohen Plaintiffs "*specifically* will be the target of any future, let alone imminent, terrorist attack." *Tomsha*, 2016 WL 3538380, at *2.

Nor can the Cohen Plaintiffs rescue their claims by arguing that they suffer a present harm resulting from their fear of such attacks, as "allegations of a subjective [fear] are not an adequate substitute for a claim of specific present objective harm or threat of a specific future harm." *Clapper*, 133 S.Ct. at 1152 (quoting *Laird v. Tatum*, 408 U.S. 1, 13–14, 92 S.Ct. 2318, 33 L.Ed.2d 154 (1972)). While the court does not question the sincerity of the Cohen Plaintiffs' anxieties, their subjective fears cannot confer standing absent a sufficient showing of the risk of future harm.[4]

---

[4] The Cohen Plaintiffs argue that they establish an injury in fact because "the Israeli statutes [that form the basis for some of their claims] were passed to protect the plaintiffs and impose a duty upon Facebook." (Pls. Mem. in Opp'n to MTD ("Opp'n Mem.") (Dkt. 29), No. 16–CV–4453, at 40.) Their argument appears to be that Israeli law gives rise to a cognizable injury in fact by creating a protected interest. However, the presence of a statutory right does not itself satisfy Article III's injury in fact requirement, which must be met in all cases. *See* Lujan, 504 U.S. at 576–78, 112 S.Ct. 2130. Where, as here, the examining court finds that plaintiffs fail to establish a constitutionally cognizable injury in fact, the resulting jurisdictional defect is not remedied by the presence of a statutory right. *See Spokeo, Inc. v. Robbins*, ___ U.S. ___, 136 S.Ct. 1540, 1549, 194 L.Ed.2d 635 (2016) ("Article III

For the foregoing reasons, the Cohen Complaint is dismissed without prejudice in its entirety. *See Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 54-55 (2d Cir. 2016) ("[W]here a complaint is dismissed for lack of Article III standing, the dismissal must be without prejudice. . . .").

B. Personal Jurisdiction

Facebook also argues that subjecting it to personal jurisdiction in New York as to the Force[5] claims would be inconsistent with state law requirements and due process principles. (*See* MTD Mem. at 22–30.) The court concludes that personal jurisdiction over Facebook is proper based on the Force Complaint's ATA-based claims, which permit a court to exercise jurisdiction over a defendant who has minimum contacts with the United States, and the doctrine of pendent personal jurisdiction. Accordingly, the court declines to dismiss the Force Complaint on this basis.

---

standing requires a concrete injury even in the context of a statutory violation.").

[5] Facebook's argument against personal jurisdiction is also directed at the Cohen Complaint and raises a number of valid but vexing questions as to the interaction between New York's statutory scheme for extending jurisdiction over corporations and recent Supreme Court decisions concerning due process limitations on personal jurisdiction. (*See* MTD Mem. at 27–30.) Because the court has determined that the Cohen Plaintiffs fail to establish standing, it need not address the question of personal jurisdiction as to their Complaint. *Cf. Ruhrgas AG*, 526 U.S. at 583–84, 119 S.Ct. 1563 (holding that subject matter questions may be, but are not necessarily, decided before questions of personal jurisdiction).

1. Legal Standard

Personal jurisdiction refers to a "court's power to exercise control over the parties." *Leroy v. Great W. United Co.*, 443 U.S. 173, 180, 99 S.Ct. 2710, 61 L.Ed.2d 464 (1979). "In order to survive a motion to dismiss for lack of personal jurisdiction, a plaintiff must make a *prima facie* showing that jurisdiction exists." *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL* ("*Licci III*"), 732 F.3d 161, 167 (2d Cir. 2013) (internal quotation marks and citation omitted). "Prior to discovery, a plaintiff may defeat a motion to dismiss based on legally sufficient allegations of jurisdiction." *In re Magnetic Audiotape Antitrust Litig.*, 334 F.3d 204, 206 (2d Cir. 2003) (citation omitted). In evaluating the sufficiency of the jurisdictional allegations, a court must "construe the pleadings and affidavits in the light most favorable to the plaintiffs, resolving all doubts in their favor." *Dorchester Fin. Secs. Inc. v. Banco BRJ, S.A.*, 722 F.3d 81, 85 (2d Cir. 2013) (internal quotation marks and citation omitted).

Establishing personal jurisdiction over a party "requires satisfaction of three primary elements": (1) procedurally proper service of process on the defendant; (2) a statutory basis for personal jurisdiction; and (3) the exercise of jurisdiction must be consistent with "constitutional due process principles." *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL* ("*Licci I*"), 673 F.3d 50, 59–60 (2d Cir. 2012). Facebook does not argue that service of process was procedurally improper, and so the court's evaluation focuses on whether the exercise of personal jurisdiction is

statutorily authorized and consistent with the strictures of due process.

2. Statutory Basis for Personal Jurisdiction

"The available statutory bases [for asserting personal jurisdiction] are enumerated by Federal Rule of Civil Procedure 4(k)." *Licci I*, 673 F.3d at 59. In one of its provisions, that rule states that "[s]erving a summons or filing a waiver of service establishes personal jurisdiction over a defendant . . . when authorized by a federal statute." Fed. R. Civ. P. 4(k)(1)(C). Where a federal statute authorizes nationwide service of process, this provision permits the exercise of personal jurisdiction over parties properly served anywhere in the United States. *See Kidder, Peabody & Co., Inc. v. Maxus Energy Corp.*, 925 F.2d 556, 562 (2d Cir. 1991) (stating nationwide service provision of the Securities Exchange Act "confers personal jurisdiction over a defendant who is served anywhere within the United States").

The Force Plaintiffs argue that the service provision of the ATA provides the statutory basis for exercising personal jurisdiction over Facebook. (Pls. Mem. in Opp'n to MTD ("Opp'n Mem.") (Dkt. 29), No. 16–CV–4453, at 7–8). In pertinent part, the relevant statute states that, for civil enforcement of federal antiterrorism statutes pursuant to 18 U.S.C. § 2333, "[p]rocess . . . may be served in any district where the defendant

resides, is found, or has an agent."[6] 18 U.S.C. § 2334(a). Various opinions, including two recent decisions from this district, have held that this provision authorizes nationwide service of process and so provides personal jurisdiction over defendants who are properly served anywhere in the United States. *Weiss v. Nat'l Westminster Bank PLC*, 176 F.Supp.3d 264, 284 (E.D.N.Y. 2016); *Strauss v. Credit Lyonnais, S.A.*, 175 F.Supp.3d 3, 26–27 (E.D.N.Y. 2016); *see also Licci I*, 673 F.3d at 59 n.8 (2d Cir. 2012) (noting the ATA's service provision as a potential basis for establishing personal jurisdiction).

Facebook does not argue that service was defective, nor does it contest the holdings in the cases cited above other than to argue that they were wrongly decided. Given the unanimity of opinion on the subject, including within the Second Circuit, and the clear language of the statute, there are no apparent grounds to disagree with Plaintiffs' position. Accordingly, the

---

[6] Immediately before its service provision, Section 2334 states that "[a]ny civil action under section 2333 . . . may be instituted in the district court of the United States for any district where any plaintiff resides or where any defendant resides or is served, or has an agent." 18 U.S.C. § 2334(a). At least one prior opinion restricted nationwide service to instances in which this venue requirement is satisfied. *See Wultz v. Islamic Rep. of Iran*, 762 F.Supp.2d 18, 25–29 (D.D.C. 2011). Facebook's apparent concession that it was properly served in the Southern District of New York prior to transfer to this court is also sufficient to establish that statutory venue was proper and so that the statutory prerequisite for nationwide service was satisfied. *Cf. Wultz*, 762 F.Supp.2d at 29–30; *Weiss v. Nat'l Westminster Bank PLC*, 176 F.Supp.3d 264, 284 n.10 (E.D.N.Y. 2016).

court finds that the ATA provides statutory grounds for extending personal jurisdiction over Facebook.

3. Due Process Considerations

Even where statutorily authorized, the exercise of personal jurisdiction must be consistent with constitutional due process requirements. *See, e.g.*, *Waldman v. Palestine Liberation Org.*, 835 F.3d 317, 327–28 (2d Cir. 2016). The reviewing court must satisfy itself that "maintenance of a lawsuit does not offend 'traditional notions of fair play and substantial justice.'" *Id.* at 328 (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316, 66 S.Ct. 154, 90 L.Ed. 95 (1945)).

While the required analysis typically looks to a party's "minimum contacts" with the particular state in which the examining court sits, satisfaction of due process as to federal statutes with nationwide service provisions depends only on a party's contact with the United States *as a whole*. *See. e.g.*, *In re Terrorist Attacks on Sept. 11, 2001*, 349 F.Supp.2d 765, 806 (S.D.N.Y. 2005); *cf. Mariash v. Morrill*, 496 F.2d 1138, 1143 (2d Cir. 1974) (noting that personal jurisdiction predicated on nationwide service "remains subject to the constraints of the Due Process clause of the *Fifth* Amendment" (emphasis added)). The First Circuit explained the basis for this distinction, stating: "Inasmuch as the federalism concerns which hover over the jurisdictional equation in a diversity case are absent in a federal question case, a federal court's power to assert personal jurisdiction is geographically expanded."

United Elec. Radio, and Mach. Workers of Am. v. 163 Pleasant St. Corp., 960 F.2d 1080, 1085 (1st Cir. 1992).

Applying this reasoning to the ATA's nationwide service provision, courts have consistently held that defendants are subject to personal jurisdiction for civil claims under that act where they have minimum contacts with the United States as a whole.[7] *See Waldman*, 835 F.3d at 331–334 (assessing personal jurisdiction based on defendants' contacts with the United States as a whole); *Strauss*, 175 F.Supp.3d at 28; *Weiss*, 176 F.Supp.3d at 285; *In re Terrorist Attacks*, 349 F.Supp.2d at 810–11.

There is no question that Facebook has the required contacts with the United States as a whole. The Force Plaintiffs allege—and Facebook does not dispute—that Facebook is incorporated in Delaware and

---

[7] Facebook argues that the ATA cases noted here are distinguishable on the basis that they apply only to foreign defendants, a distinction they claim has legal salience because "any American defendants would have very different federalism-backed expectations than a foreign defendant about where in the United States it may be hailed into court." (Def. Reply in Further Supp. of MTD ("Reply Mem.") (Dkt. 31), No. 16–CV–4453, at 9.) However, Facebook cites no authority that supports this restriction and, though it is correct that analysis of minimum contacts and personal jurisdiction under the ATA has been limited to foreign parties, courts in this circuit have applied the same rule to US-based defendants under other laws with similar provisions. *See. e.g.*, *Local 8A-28A Welfare and 401(k) Retirement Funds v. Golden Eagles Architectural Metal Cleaning and Refinishing*, 277 F.Supp.2d 291, 294 (S.D.N.Y. 2003); *Hallwood Realty Partners, L.P. v. Gotham Partners, L.P.*, 104 F.Supp.2d 279, 281–87 (S.D.N.Y. 2000). Accordingly, the court finds no reasons to treat this distinction as controlling here.

has its principal place of business in California. (Force FAC ¶ 19.) As a United States resident, Facebook could hardly argue that it lacks the required contacts with the country as a whole. *Mariash*, 496 F.2d at 1143 ("[W]here, as here, the defendants reside within the territorial boundaries of the United States, the 'minimal contacts,' required to justify the federal government's exercise of power over them, are present."); *cf. Daimler AG v. Bauman*, ___ U.S. ___, 134 S.Ct. 746, 760, 187 L.Ed.2d 624 (2014) (holding that a corporation is "fairly regarded at home" and so "amenable" to personal jurisdiction for suits relating to all of its activities, including those outside the forum, in its principal place of business and place of incorporation). Accordingly, the court finds that exercising of jurisdiction over Facebook with respect to the ATA claims comports with the requirements of due process.

4. Pendent Personal Jurisdiction[8]

"A plaintiff must establish the court's jurisdiction with respect to *each* claim asserted" *Sunward Elec., Inc. v. McDonald*, 362 F.3d 17, 24 (2d Cir. 2004), and so

[8] The Court does not address the potential state law bases for extending personal jurisdiction over the Force Plaintiffs' remaining claims, nor it is required to do so where pendent personal jurisdiction is available. *IUE AFL-CIO Pension Fund v. Herrmann*, 9 F.3d 1049, 1057 (2d Cir. 1993) ("We need not reach the question whether personal jurisdiction as to the state law claims was otherwise available because the district court had personal jurisdiction over the defendants under [a statute with a nationwide service of process provision] and the state law claims derive from a common nucleus of operative facts with the federal claims.")

the court is required to assess personal jurisdiction as to the Force Complaint's remaining, Israeli law-based claims.

"[U]nder the doctrine of pendent personal jurisdiction, where a federal statute authorizes nationwide service of process, and the federal and [non-federal] claims 'derive from a common nucleus of operative fact', the district court may assert personal jurisdiction over the parties to the related [] claims even if personal jurisdiction is not otherwise available." *IUE AFL–CIO Pension Fund v. Herrmann*, 9 F.3d 1049, 1056 (2d Cir. 1993) (internal quotation marks and citations omitted). A common nucleus of operative fact exists between claims where "the facts underlying the federal and [non-federal] claims substantially overlap[] [or] the federal claim necessarily [brings] the facts underlying the [non-federal] claim before the court." *Achtman v. Kirby, McInerney & Squire, LLP*, 464 F.3d 328, 335 (2d Cir. 2006) (internal quotation marks and citation omitted).

District courts have discretion as to whether to exercise pendent personal jurisdiction, the exercise of which should be informed by "considerations of juridical economy, convenience, and fairness to litigants." *See In re LIBOR-Based Fin. Instruments Antitrust Litig.*, No. 11-MD-2262 (NRB), 2015 WL 6243526, at *23 (S.D.N.Y. Oct. 20, 2015) (quoting *Oetiker v. Jurid Werke, G.m.b.H.*, 556 F.2d 1, 5 (D.C. Cir. 1977)).

Those considerations strongly favor exercising pendent jurisdiction over Facebook with respect to the

Force Complaint's non-ATA-based claims. The ATA and non-ATA-based claims derive from the same underlying allegations and legal theories: that Facebook's provision of "services" to Hamas assisted that organization in recruiting, organizing, facilitating, and instigating attacks, and that Facebook failed to stop this abuse of its platform. There would be no inconvenience or unfairness to Facebook in requiring it to litigate the same facts before the same court, nor would splitting up the claims between multiple courts do anything to conserve judicial resources. In view of the foregoing discussion of the ATA's nationwide service provision, the court exercises personal jurisdiction over Facebook with respect to the Force Plaintiffs' remaining claims as well.

* * *

Accordingly, the court concludes that Facebook is subject to personal jurisdiction in New York as to the claims asserted in the Force Complaint, and denies its motion to dismiss for lack of personal jurisdiction.

C. Failure to State a Claim Based on the Communications Decency Act[9]

The parties dedicate much of their briefing debating the applicability of Section 230(c)(1) of the

[9] Facebook separately seeks dismissal of the Force Complaint's federal law-based causes of action, arguing that the Force Plaintiffs fail to state a plausible claim for relief under the applicable statutes. (MTD Mem. at 32–40.) The court does not address this argument, as it concludes that all of the Force Complaint's claims must be dismissed on the basis of the Communications Decency Act.

Communications Decency Act ("Section 230(c)(1)") to the present dispute. There are two distinct species of arguments regarding Section 230(c)(1) raised in the parties' briefs. First, the parties dispute whether the asserted claims fall within the substantive coverage of Section 230(c)(1). Second, the Force Plaintiffs argue that Facebook is improperly attempting to apply Section 230(c)(1) extraterritorially. The court considers these arguments separately and concludes that the activity alleged falls within the immunity granted by Section 230(c)(1) and that application of that subsection to the present dispute is not impermissibly extraterritorial.

1. Legal Standard

The purpose of a motion to dismiss for failure to state a claim under Rule 12(b)(6) is to test the legal sufficiency of a plaintiff's claims for relief. *Patane v. Clark*, 508 F.3d 106, 112 (2d Cir. 2007). In reviewing a complaint on such a motion, the court must accept as true all allegations of fact, and draw all reasonable inferences in favor of the plaintiff. *ATSI Commc'ns, Inc. v. Shaar Fund Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007). A complaint will survive a motion to dismiss if it contains "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). However, even where a claim is otherwise plausible, a defendant may move to dismiss based on an available

affirmative defense, and the court may grant the motion on that basis "if the defense appears on the face of the complaint." *Pani v. Empire Blue Cross Blue Shield*, 152 F.3d 67, 74 (2d Cir. 1998); *see also Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015).

2. Coverage of Section 230(c)(1)

a. Overview of Section 230(c)(1)

Section 230(c)(1) shields defendants who operate certain internet services from liability based on content created by a third party and published, displayed, or issued through the use of the defendant's services. That subsection states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1).

The Second Circuit recently described the necessary components of an immunity claim under Section 230(c)(1), stating that the law "shields conduct if the defendant (1) is a provider or user of an interactive computer service, (2) the claim is based on information provided by another information content provider and (3) the claim would treat [the defendant] as the publisher or speaker of that information." *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016) (alteration in original) (internal quotation marks and citations omitted). Where a defendant establishes these requirements based on the face of a complaint, a motion to dismiss may be granted. *See Ricci*, 781 F.3d

at 28 (citing *Klayman v. Zuckerberg*, 753 F.3d 1354, 1357 ("*Klayman II*") (D.C. Cir. 2014)).

The Force Plaintiffs do not genuinely contest that the first and second elements of this test are satisfied in the present case,[10] but rather focus their efforts on contesting the final requirement for obtaining Section 230(c)(1) immunity—that "the claim would treat [the defendant] as the publisher or speaker of" third party content. Under this prong, qualifying defendants are protected from liability predicated on their "exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content" that they did not themselves create. *LeadClick Media*, 838 F.3d at 174 (internal quotation marks

---

[10] While the court does not engage in an extended discussion of the first two prongs here, Facebook and the content at issue qualify easily. The Second Circuit has not considered whether social media platforms in particular are "interactive computer services" within the meaning of the law; however, other courts have readily concluded that such websites (and Facebook in particular) fall into this category. *See. e.g.*, *Klayman II*, 753 F.3d at 1357–58; *Doe v. MySpace, Inc.*, 528 F.3d 413, 420–22 (5th Cir. 2008). With regard to the second prong—that the "claim is based on information provided by another content provider"—the Second Circuit has indicated that a defendant falls afoul of this requirement only where "it assisted in the development of what made the content unlawful." *LeadClick Media*, 838 F.3d at 174. The District Court for the District of Columbia recently rejected an argument that Facebook fell afoul of this standard by using data collected from users to suggest other content and users, stating that "the manipulation of information provided by third parties does not automatically convert interactive service providers into information content providers." *Klayman v. Zuckerberg*, 910 F.Supp.2d 314, 321 n.3 ("*Klayman I*") (D.D.C. 2012), *aff'd*, 753 F.3d 1354 (D.C. Cir. 2014).

and citation omitted). The Second Circuit's most recent opinion on the subject provided the following guidance as to when a defendant is shielded:

> [W]hat matters is whether the cause of action inherently requires the court to treat the defendant as the "publisher or speaker" of content provided by another. To put it another way, courts must ask whether the duty that the plaintiff alleges the defendant violated *derives from the defendant's status or conduct as a "publisher or speaker.*"

Id. at 175 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102 (9th Cir. 2009)) (emphasis added). This guidance emphasizes that Section 230(c)(1) is implicated not only by claims that explicitly point to third party content but also by claims which, though artfully pleaded to avoid direct reference, implicitly require recourse to that content to establish liability or implicate a defendant's role, broadly defined, in publishing or excluding third party Communications. *See, e.g.*, *Jane Doe No. 1 v. Backpage.com,* LLC, 817 F.3d 12, 19 (1st Cir. 2016) ("The ultimate question [of whether Section 230(c)(1) applies] does not depend on the form of the asserted cause of action. . . .") (collecting cases); *Manchanda v. Google*, No. 16-CV-3350 (JPO), 2016 WL 6806250, at *2 (S.D.N.Y. Nov. 16, 2016).

In keeping with this expansive view of the publisher's role, judicial decisions in the area consistently stress that decisions as to whether existing content should be removed from a website fall within the editorial prerogative. *See Ricci*, 781 F.3d at 28; *Klayman*

II, 753 F.3d at 1359; *Green v. Am. Online (AOL)*, 318 F.3d 465, 471 (3d Cir. 2003) ("[D]ecisions relating to the monitoring, screening, and deletion of content from [defendant's] network . . . quintessentially relate[ ] to a publisher's role."); *Barnes*, 570 F.3d at 1103 ("[R]emoving content is something publishers do."). Similarly, a recent opinion found that decisions as to the "structure and operation" of a website also fall within Section 230(c)(1)'s protection, *Backpage.com*, 817 F.3d at 21, a determination which one court extended to a social media platform's decisions as to who may obtain an account, *see Fields v. Twitter*, 217 F.Supp.3d 1116, 1123–24, No. 16-CV-213, 2016 WL 6822065, at *6 ("*Fields II*") (N.D. Cal. Nov. 18, 2016).

b. Application

While the Force Plaintiffs attempt to cast their claims as content-neutral, even the most generous reading of their allegations places them squarely within the coverage of Section 230(c)(1)'s grant of immunity. In their opposition to the present motion, the Force Plaintiffs argue that their claims seek to hold Facebook liable for "provision of services" to Hamas in the form of account access "coupled with Facebook's refusal to use available resources . . . to identify and shut down Hamas [ ] accounts." (Opp'n Mem. at 27; *see also* Force FAC ¶¶ 543–55.) While superficially content-neutral, this attempt to draw a narrow distinction between policing accounts and policing content must ultimately be rejected. Facebook's choices as to who may use its platform are inherently bound up in its

decisions as to what may be said on its platform, and so liability imposed based on its failure to remove users would equally "derive[ ] from [Facebook's] status or conduct as a 'publisher or speaker.'" *LeadClick Media*, 838 F.3d at 175 (internal quotation marks and citations omitted). Section 230(c)(1) prevents courts from entertaining civil actions[11] that seek to impose liability on defendants like Facebook for allowing third parties to post offensive or harmful content or failing to remove such content once posted. *See Ricci*, 781 F.3d at 28; *Klayman II*, 753 F.3d at 1359 ("[T]he very essence of publishing is making the decision whether to print or retract a given piece of content."). For the same reason, it is clear that Section 230(c)(1) prevents the necessarily antecedent editorial decision to allow certain parties to post on a given platform, as that decision cannot be meaningfully separated from "choices about

---

[11] The Force Plaintiffs also refer in passing to a subsection of Section 230 which states that "[n]othing in this section shall be construed to impair the enforcement of . . . any [ ] Federal criminal statute." 47 U.S.C. § 230(e)(1). (Opp'n Mem. at 26–27.) While, read most favorably, this section could be interpreted to inhibit immunity as to civil liability predicated on federal criminal statutes, such as the ATA provisions at issue here, this reading has been rejected by most courts that have examined it. *See Backpage.com*, 817 F.3d at 23; *M.A. ex rel P.K. v. Vill. Voice Media Holdings, LLC*, 809 F.Supp.2d 1041, 1054–55 (E.D. Mo. 2011); *Doe v. Bates*, No. 5:05-CV-91, 2006 WL 3813758, at *3–4 (E.D. Tex. Dec. 27, 2006); *Obado v. Magedson*, No. 13-cv-2382, 2014 WL 3778261 (D.N.J. July 31, 2014); *but see Nieman v. Versuslaw, Inc.*, No.12–3104, 2012 WL 3201931, at *9 (C.D. Ill. Aug. 3, 2012). The court concludes that this subsection does not limit Section 230(c)(1) immunity in civil actions based on criminal statutes but rather extends only to criminal prosecutions.

what [third party] content can appear on [the platform] and in what form." *Fields II*, 217 F.Supp.3d at 1124, 2016 WL 6822065, at *6 (quoting *Backpage.com*, 817 F.3d at 20–21).

Further, it is clear that the Force Plaintiffs' claims are not based solely on the provision of accounts to Hamas but rely on content to establish causation and, by extension, Facebook's liability. The essence of the Force Complaint is not that Plaintiffs were harmed by Hamas's ability to obtain Facebook accounts but rather by its use of Facebook for, *inter alia*, "recruiting, gathering information, planning, inciting, [ ] giving instructions for terror attacks, . . . issu[ing] terroristic threats, . . . [and] intimidating and coerc[ing] civilian populations." (Force FAC ¶ 112; *see also* Opp'n Mem. at 29 ("[P]laintiffs have alleged how Facebook's provision of services and resources to Hamas substantially contributed to Hamas's ability to carry out the attacks at issue and the attacks were a foreseeable consequence of the support provided by Facebook.") Said differently, the Force Plaintiffs claim that Facebook contributed to their harm by allowing Hamas to use its platform to post particular offensive *content* that incited or encouraged those attacks. Facebook's role in publishing that content is thus an essential causal element of the claims in the Force Complaint, and allowing liability to be imposed on that basis would "inherently require[ ] the court to treat the defendant as the publisher or speaker of content provided by" Hamas. *LeadClick Media*, 838 F.3d at 175 (internal quotation marks and citations omitted); *see also Fields II*, 217 F.Supp.3d at

1124, 2016 WL 6822065, at *7 ("Although plaintiffs have carefully restructured their [complaint] to focus on their provision of accounts theory of liability, at their core, plaintiffs' allegations are still that [the social media platform] failed to prevent [terrorists] from disseminating content through [its] platform, not its mere provision of accounts. . . .").

Accordingly, the court finds that the Force Plaintiffs' claims against Facebook fall within the scope of Section 230(c)(1)'s grant of immunity. The court proceeds to consider whether that statute may be applied to the present dispute.

3. Extraterritorial Application of the Communications Decency Act

Separate from its substantive scope, the Force Plaintiffs argue that Section 230(c)(1) does not apply to the present dispute because, under the presumption against extraterritoriality, it cannot be applied to conduct that occurs wholly outside of the United States. (*See* Opp'n Mem. at 30–31.) Pointing to recent Supreme Court holdings, Plaintiffs claim that because "the CDA 'gives no clear indication of an extraterritorial application,' under [*Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247 [130 S.Ct. 2869, 177 L.Ed.2d 535] (2010)], the CDA has no extraterritorial application." (*Id.* at 31.)

a. Overview of the Presumption against Extraterritoriality

Based on the premise that "United States law governs domestically but does not rule the world," the presumption against extraterritoriality dictates that statutes should only be given domestic effect absent a definitive demonstration of Congress's intent for them to apply abroad. *See RJR Nabisco, Inc. v. European Cmty.,* ___ U.S. ___, 136 S.Ct. 2090, 2100, 195 L.Ed.2d 476 (2016) (internal quotation marks and citations omitted). While "the presumption against extraterritoriality is 'typically' applied to statutes 'regulating conduct,'" *id.* at 2100 (quoting *Kiobel v. Roval* [sic] *Dutch Petroleum*, 569 U.S. 108, 133 S.Ct. 1659, 1664, 185 L.Ed.2d 671 (2013)), the Supreme Court recently clarified that, "regardless of whether the statute in question regulates conduct, affords relief, or merely confers jurisdiction," all questions of extraterritoriality should be assessed using a "two-step framework," *id.* at 2101.

The first step requires the court to determine "whether the statute gives a clear, affirmative indication that it applies extraterritorially." *Id.* The presumption against extraterritoriality does not apply if a statute contains an express demonstration of Congress's intent that the law should apply abroad. *See Morrison*, 561 U.S. at 255, 130 S.Ct. 2869. Conversely, absent evidence of such intent, the statute can only be applied domestically. *Id.* ("[W]hen a statute gives no clear indication of extraterritorial application, it has none.")

If a statute lacks clear indicia of intended extraterritorial effect, the examining court must then "determine whether the case at issue involves [] a prohibited [extraterritorial] application" of the law. *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* ("*Microsoft Corp.*"), 829 F.3d 197, 216 (2d Cir. 2016). Accomplishing this step requires the court to identify the "focus" of the statute, defined as the "objects of the statute's solicitude." *Morrison*, 561 U.S. at 267, 130 S.Ct. 2869. From this, the court must distill the relevant "territorial events or relationships" that bear on that "focus," *see Microsoft Corp.,* at 216 (internal citation omitted), separating those events whose location is relevant to the statute's central emphasis from those that are peripheral. The final element of this analysis requires the court to assess whether the relevant "territorial events and relationships" occurred domestically or abroad with respect to the challenged application of the statute. *Id.* If, in the final analysis, the court determines that "the domestic contacts presented by the case fall within the 'focus' of the statutory provision or are 'the objects of the statute's solicitude,' then the application of the provision is not unlawfully extraterritorial." *Id.* (quoting *Morrison*, 561 U.S. at 267, 130 S.Ct. 2869).

b. Application to Section 230(c)(1)

i. Indicia of Section 230(c)(1)'s Intended Extraterritorial Effect

No other court appears to have addressed the presumption against extraterritoriality in the context of a statute which limits liability or imparts immunity. At the outset, the court agrees with the Force Plaintiffs that the statute itself lacks an "affirmative indication that it applies extraterritorially," *RJR Nabisco*, 136 S.Ct. at 2101, as none of Section 230(c)(1), the surrounding provisions, or any other section of the Communications Decency Act demonstrate any clear consideration of such application, see Communications Decency Act of 1996, Pub. L. No. 104–104, 110 Stat 56, §§ 501–61 (codified in scattered sections of Title 18 and Title 47 of the United States Code).

ii. Determining the Statutory "Focus"

Moving on to find the statute's "focus," the court concludes that the "object[ ] of [Section 230(c)(1)'s] solicitude" is its limitation on liability. *Morrison*, 561 U.S. at 267, 130 S.Ct. 2869. In drawing this conclusion, the court turns "to the familiar tools of statutory interpretation," *Microsoft Corp.*, 829 F.3d at 217, determining the relevant provision's focus by examining its text and context.

Looking first to the plain language of Section 230(c)(1), the court concludes that the "most natural reading of [that provision] . . . suggests a legislative focus on" providing immunity. *Id.* Section 230(c)(1)

offers only one directive—that qualifying defendants may not be treated as the "publisher or speaker of any" third party content—which it does not cabin based on either the location of the content provider or the user or provider of the interactive computer service. 47 U.S.C. § 230(c)(1). This emphasis on immunity over other considerations is clear from the text, and courts interpreting that provision have consistently found Section 230(c)(1)'s plain language focuses on protecting qualified defendants from civil suits. *See. e.g.*, *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

Viewing the relevant language in the context of the surrounding provisions and the policy goals of that section further supports this view of its "focus." Other than the relevant provision, Section 230 contains only two other substantive provisions, one of which is similarly explicit in limiting civil liability for providers and users of interactive computer services.[12] 47 U.S.C. § 230(c)(2). Both of these immunizing provisions were adopted specifically for the purpose of clarifying—and curtailing—the scope of internet-providing defendants' exposure to liability predicated on third party content,[13] and much of the surrounding statutory

---

[12] Section 230 also requires interactive computer service providers to provide notice to customers of commercially available parental control products that allow for content limitations. 47 U.S.C. § 230(d).

[13] Notes of debates around the adoption of the precise language at issue demonstrate that Congress acted with the purpose of limiting liability. *See* H.R. Rep. No. 104–458, at 194H.R. Rep. No. 104–458, at 194 (1996) (H.R. Conf. Rep.), *reprinted in* 1996

language emphasizes and supports this focus. This is evidenced, for instance, by Section 230's stated purpose of preserving an open and free internet uninhibited by external limitations, *see* 47 U.S.C. § 230(b)(2), and its listed exceptions to the broad liability provided therein, *see id.* § 230(e).

iii. Ascertaining the Relevant "Territorial Events and Relationships"

In light of its focus on limiting civil liability, the court concludes that the relevant location is that where

---

U.S.C.C.A.N. 10. The court observes, however, that the legislative intent is not unequivocal in this regard. The provision at issue was adopted in response to a New York case, *Stratton Oakmont Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which held an internet service provider liable for the comments by its users, concluding that the service provider became a "publisher" by virtue of having selectively removed content and so was subject to liability for republishing defamatory comments that it had not removed. *Id.* at *3–4. In overruling that decision, Congress evidently sought to remove disincentives to selective removal of material created by that opinion, which it concluded would impair "the important federal policy of empowering parents to determine the content of Communications their children receive through interactive computer service." H.R. Rep. No. 104–458 at 194H.R. Rep. No. 104–458 at 194. Some opinions have noted that the subsequent interpretation of the law, which arguably undermines information service providers' incentives to remove any information by inculcating them against liability for the content they display, overreads the protections that Congress sought to provide. *See Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 669–70 (7th Cir. 2008). Whatever the merits of that argument, for present purposes it is relevant only to show that Congress's "focus" in including the relevant language was on limiting liability, not its reasons for adopting that policy.

the grant of immunity is applied, i.e. the situs of the litigation. Section 230(c)(1) suggests a number of "territorial relationships and events," which are generally divisible into those associated with the underlying claim (e.g., the location of the information content provider, the internet service provider, or the act of publishing or speaking) and the location associated with the imposition of liability, i.e. where the internet service provider is to be "treated" as the publisher or speaker. Given the statutory focus on limiting liability, however, the location of the relevant "territorial events" or "relationships" cannot be the place in which the claims arise but instead must be where redress is sought and immunity is needed.

With this in mind, the court concludes that the Force Action does not require an impermissible extraterritorial application of Section 230(c)(1). As the situs of the litigation is New York, the relevant "territorial events or relationships" occur domestically. Accordingly, the court rejects the Force Plaintiff's argument that Facebook should be denied immunity under Section 230(c)(1).[14]

---

[14] The Force Plaintiffs separately claim that Section 230(c)(1) does not apply to claims based in foreign law (Opp'n Mem. at 31), and argue that their Israeli tort law claims are properly before the court under a conflict of laws analysis (*id.* at 31–36). Their argument that the Communications Decency Act does not limit Israeli law claims is apparently based on lack of any reference to foreign law in the Section 230's subsection entitled "Effect on other laws." 47 U.S.C. § 230(e). The relevant subsection provides a limited list of exceptions to Section 230(c)'s limitations on liability. *See, e.g.*, *id.* §§ 230(e)(1) (stating that the liability provisions

* * *

Accordingly, the court grants Facebook's motion to dismiss all claims in the Force Complaint for failure to state a claim upon which relief can be granted.

IV. CONCLUSION

For the foregoing reasons, Facebook's Motions to Dismiss ((Dkt. 23), No. 16–CV–4453; (Dkt. 34), No. 16–CV–5158) are GRANTED. The Amended Complaint in the Cohen Action (Dkt. 17), No. 16–CV–4453) is DISMISSED WITHOUT PREJUDICE. The Amended Complaint in the Force Action ((Dkt. 28), No. 16–CV–5158) is DISMISSED WITHOUT PREJUDICE. The Clerk of Court is respectfully DIRECTED to enter judgment accordingly.

SO ORDERED.

---

do not impair enforcement of federal criminal laws), 230(e)(3) (stating that Section 230 does not affect state laws that are "consistent with this section"). The Force Plaintiffs argue that failing to include foreign law in this section indicates that Section 230(c)(1)'s grant of immunity does not apply to Israeli law-based claims. The court disagrees and understands the significance of this omission to be just the opposite: because there is no listed exception for foreign law claims, those claims remain subject to the limitations on liability provided by Section 230(c)(1). *Cf. TRW Inc. v. Andrews*, 534 U.S. 19, 28, 122 S.Ct. 441, 151 L.Ed.2d 339 (2001) ("Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent." (internal quotation marks and citations omitted)).

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 29th day of August, two thousand nineteen.

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

ORDER

Docket No: 18-397

(Filed Aug. 29, 2019)

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.

Appellants filed a petition for panel rehearing, or, in the alternative, for rehearing *en banc*. The panel that determined the appeal has considered the request

for panel rehearing, and the active members of the Court have considered the request for rehearing *en banc*.

IT IS HEREBY ORDERED that the petition is denied.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk

[SEAL]

/s/ Catherine O'Hagan Wolfe

47 U.S.C.A. § 230. Protection for private blocking and screening of offensive material

Effective: April 11, 2018

(a) Findings

The Congress finds the following:

(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.

(b) Policy

It 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;

(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;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No 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 paragraph (1).[1]

(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

---

[1] So in original. Probably should be "subparagraph (A)".

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section 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.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(5) No effect on sex trafficking law

Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit –

(A) any claim in a civil action brought under section 1595 of Title 18, if the conduct

underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of Title 18; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of Title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

(f) Definitions

As used in this section:

(1) Internet

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

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.

(4) Access software provider

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.