No. 16-17165

IN THE

United States Court of Appeals

FOR THE NINTH CIRCUIT

TAMARA FIELDS, ET AL.,

Plaintiffs-Appellants,

v.

TWITTER, INC.,

Defendant-Appellee.

On Appeal from the United States District Court
for the Northern District of California
District Court No. 3:16-cv-00213-WHO
The Honorable William H. Orrick

BRIEF OF *AMICUS CURIAE* INTERNET ASSOCIATION IN SUPPORT OF DEFENDANT-APPELLEE TWITTER, INC.

SONALI D. MAITRA
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666
smaitra@durietangri.com

Counsel for Amicus Curiae Internet Association

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Internet Association has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.

DATED: June 7, 2017

/s/ Sonali D. Maitra

Sonali D. Maitra
DURIE TANGRI LLP
Counsel for Amicus Curiae Internet Association

CERTIFICATE OF COMPLIANCE WITH RULE 29(C)(5)

Counsel for the parties did not author this brief in whole or in part. The parties have not contributed money intended to fund preparing or submitting the brief. No person other than *Amicus Curiae* (including our members) or our counsel contributed money to fund preparation or submission of this brief.

DATED: June 7, 2017

/s/ Sonali D. Maitra

Sonali D. Maitra
DURIE TANGRI LLP
Counsel for Amicus Curiae Internet Association

TABLE OF CONTENTS

PAGE NO.

TABLE OF AUTHORITIES

PAGE NO(S).

Cases

Statutes

Other Authorities

IDENTITY AND INTEREST OF THE *AMICUS CURIAE*

Amicus Curiae Internet Association is a nonprofit trade organization representing the interests of the world's leading Internet companies and their global community of users. We are dedicated to advancing public policy solutions to foster innovation and economic growth and empower users. Our membership includes Amazon.com, eBay, Expedia, Facebook, Google, IAC, LinkedIn, Monster Worldwide, Rackspace, salesforce.com, TripAdvisor, Twitter, and Zynga.[1] As stated, neither Twitter nor counsel for Twitter authored this brief in whole or in part.

Our members have substantial interest in the rules governing liability for unlawful and offensive content generated by third parties and circulated through online platforms. Over the past several years, courts across the country, including this one, have held that Section 230 of the Communications Decency Act (47 U.S.C. § 230) affords interactive service providers like Twitter and our members broad immunity for such third-party content. The district court's decision is in line with that precedent. Overturning this decision would substantially undermine the immunity afforded by Section 230 and the policies underlying it.

---

[1] A full list of Internet Association members may be found on our website at https://internetassociation.org/our-members/

CONSENT OF THE PARTIES

Counsel for Defendant-Appellee Twitter, Inc. ("Twitter"), consented to the filing of this brief. Counsel for Plaintiffs-Appellants Tamara Fields, *et al.* ("Appellants"), declined to consent. *Amicus Curiae's* motion for leave to file this *Amicus* Brief is filed concurrently herewith.

I. SUMMARY OF ARGUMENT

We have genuine and unconditional sympathy for the families of Lloyd Fields and James Creach—as well as for any victims of senseless violence anywhere in the world. We agree with Appellants that ISIS's hate, brutality, and crimes against humanity have no place in our society, and certainly no place on our members' services.

Appellants ask to hold Twitter liable for unlawful and offensive content generated by third parties and circulated through its platform. But Congress has already spoken on this issue in passing Section 230 of the Communications Decency Act—and the district court properly held that Section 230 prevented Appellants from pursuing their case against Twitter.

This Court is no stranger to Section 230. Section 230 affords broad, bright-line immunity to interactive computer service providers like Twitter from liability for harm resulting from third-party activity on their sites. Congress made explicit the policies it sought to advance with this immunity, including to "promote the continued development of the Internet and other interactive computer services" while, at the same time, to "remove disincentives for the development and utilization of blocking and filtering technologies . . . ." 47 U.S.C. § 230(b). Section 230 therefore was not only about immunizing intermediaries so that the Internet could thrive and grow; it was also a clear policy choice on how

best to encourage intermediaries like Twitter and our members to take their own steps to regulate offensive content on their sites.

Congress reasoned that without such immunity, Internet companies might not choose to remove content on their site, fearful of an unrelenting stream of liability for having knowledge of content they could never perfectly monitor, no matter how much they tried. Or, at the other extreme, Internet companies might vastly limit the availability of their services to allow for complete review of all content ever posted. Congress decided that neither option was acceptable. It made the express policy choice that imposing liability on the service providers that host speech was ***not*** the right way to deter harmful online speech.

In the sections that follow, we make three fundamental points: (1) everyone involved in cases like this one shares a common goal: to keep offensive content off online services; (2) in Section 230, Congress decided that broad immunity from liability for third-party content was the best way to encourage intermediaries to tackle objectionable content on their services; and (3) the policies underlying Section 230 are at odds with Appellants' request to hold Twitter liable for providing accounts and messaging services.

II. ARGUMENT

A. Our Members Share The Goal Of Ridding Their Services Of Offensive And Dangerous Content

The thrust of Appellants' case is that the courts must afford relief because Internet companies care little about policing offensive and dangerous activity on their services. That premise is wrong.

Our members have strict rules and policies prohibiting dangerous, offensive, and terrorist content on their services. Our members work with law enforcement when encountering content that may pose a genuine risk of physical harm or a direct threat to public safety. Many of our members have teams spanning the globe—working 24 hours a day, 7 days a week—tasked with reviewing reports of content and accounts that violate their policies and rules. Terrorist accounts and content are given top priority, and are removed as soon as these members become aware of them. There are also efforts to encourage and promote "counterspeech" by moderate voices in response to extremist ones, by taking actions such as commissioning research on what makes counterspeech effective, training NGOs about best counterspeech practices, and offering incentives for certain organizations and individuals to promote their counterspeech against terrorism.

Twitter, the Appellee in this case, is no different. Not only does Twitter prohibit the use of its service to promote terrorism or make

violent threats, but it suspended over 360,000 accounts between mid-2015 and August 2016 alone for threatening or promoting terrorist acts, primarily related to ISIS. Like other companies, Twitter uses both teams that review reports of terrorist activities and proprietary technology tools to identify other potentially objectionable materials. Twitter has also joined with other Internet companies to create a shared industry database of "hashes"—unique digital fingerprints—for violent terrorist imagery or terrorist recruitment videos or images that they have removed from their services. In July 2015, former FBI Director James Comey recognized Twitter's commitment to blocking terrorist content, praising it as "very good and thoughtful and hardworking at trying to shut down [terrorism-related] accounts." Ryan J. Reilly, "If You're Trying to Join ISIS Through Twitter, the FBI Probably Knows About It," Huffington Post (Jul. 9, 2015), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html.[2]

[2] The information in this paragraph can be found on Twitter's blog, at: https://blog.twitter.com/official/en_us/a/2016/combating-violent-extremism.html; https://blog.twitter.com/official/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.html; and https://blog.twitter.com/official/en_us/a/2016/partnering-to-help-curb-the-spread-of-terrorist-content-online.html.

Given that our members (including Twitter) are all committed to preventing terrorists from using their services to spread hateful propaganda, the question raised by cases like this one is: what is the appropriate legal framework for achieving those objectives? Congress has spoken directly on this issue.

B. The Broad Protections Of Section 230 Are Meant To Encourage Self-Policing, Among Other Important Goals

In 1995, the New York Supreme Court decided *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). The court in that case held Prodigy, an early online service provider, liable for defamation based on third-party statements posted on one of its interactive sites. *Stratton* was the impetus for Section 230—Congress disagreed with both its holding and the implications for the nascent industry of online intermediaries. H.R. Rep. No. 104-458 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 10; *see also Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1163-64 (9th Cir. 2008) (en banc). That case is therefore key to understanding what Congress intended in passing Section 230, and we discuss it in detail here.

Prodigy was one of the first Internet-based social networks in the world. It operated a computer network with two million users, hosting "bulletin boards" on which third parties could post their own content. *Stratton*, 1995 WL 323710, at *1-2. Prodigy held itself out as a "family

oriented computer network" and, in pursuit of that goal, took affirmative steps to remove third-party content on its site—such as issuing "content guidelines" prohibiting insulting and grossly repugnant behavior, using a content screening program that identified offensive language, and using "Board Leaders," whose responsibility was to enforce Prodigy's content guidelines. *Id.* at *2-3.

But Prodigy's attempt to address objectionable content on its site backfired. Rather than acknowledging Prodigy's efforts to set up and enforce content guidelines, the court held Prodigy liable for defamatory third-party content on its bulletin boards *because* it made "decisions as to content" such as "actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and bad taste." *Id.* at *4 (internal quotation marks omitted) (citation omitted). The court found of no consequence the fact that the "sheer volume" of the bulletin board postings (60,000 per day) made it impractical for Prodigy to regulate every piece of content on its site—instead faulting Prodigy's partial efforts to do so. *Id.* at *3.

The court distinguished a New York federal case, *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), in which the court had held a similar online service, CompuServe, free from liability for third-party content hosted on an "electronic library" of online forums. The difference? CompuServe had "no opportunity to review the contents of the publication at issue" and had "little or no editorial

control over the contents of those publications." *Stratton*, 1995 WL 323710, at *4 (internal quotation marks omitted).

The lesson that emerged from *Stratton* and *Cubby* was that online service providers that voluntarily tried to filter some content would become liable for *all* content, whereas providers that did nothing would not. It made no difference that comprehensively reviewing all content—or getting every content decision "right"—was impossible.

The *Stratton* court justified its decision with a policy argument (based exclusively on the facts of that case and a single law review article): "For the record, the fear that this Court's finding of publisher status for PRODIGY will compel all computer networks to abdicate control of their bulletin boards, incorrectly assumes that the market will refuse to compensate a network for its increased control and the resulting increased exposure." *Id.* at *5.

It was precisely this approach, and the assumptions underlying it, that Congress *rejected* when it enacted Section 230 of the CDA the following year. *See* H.R. Rep. No. 104-458 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 10 ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material."). Section 230 is entitled "Protection for private blocking and screening of offensive material." It begins with

express congressional findings: "Internet and other interactive computer services . . . represent an extraordinary advance in the availability of educational and informational resources to our citizens," that "offer users a great degree of control . . . as well as the potential for even greater control in the future as technology develops," and that "have flourished, to the benefit of all Americans, with a minimum of government regulation." 47 U.S.C. § 230(a)(1)-(5). The statute also lists a number of policies and goals served by the subsection, including "to promote the continued development of the Internet," "to preserve the vibrant and free market that presently exists for the Internet," "to . . . maximize user control," and "to remove disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b)(1)-(5).

The product of these policies and findings is a law that creates broad-based immunity for online intermediaries. The relevant provision reads: "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 title of this subsection is: "Protection for 'Good Samaritan' blocking and screening of offensive material"—yet another indication of Congress's interest in encouraging self-policing rather than punishing it. *See*

Roommates.com, 521 F.3d at 1163-64 ("the substance of section 230(c) can and should be interpreted consistent with its caption").[3]

In enacting Section 230, Congress made a clear policy choice: the right way to both encourage the development of the Internet *and* incentivize providers to keep harmful content from their services was to immunize them from liability for third-party content. This immunity opened the door for online service providers to address harmful content without fear of inviting liability for failing to catch or remove certain objectionable content. As this Court sitting en banc explained, Congress sought to remove the "grim choice" of having to "choose between taking responsibility for all messages and deleting no messages at all." *Id.* at 1163; *see also Carafano v. Metrosplash.com Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003) (The statute is designed at once "to promote the free exchange of information and ideas over the

[3] Since Section 230 was enacted, Congress has re-affirmed its commitment to the section's principles and broad-based immunity. In 2002, Congress passed the "Dot Kids Implementation and Efficiency Act," establishing a domain for kid-appropriate material. Pub. L. No. 107-317, 116 Stat. 2766 (2002). In the statute's committee report, Congress explained that "[t]he courts have correctly interpreted section 230(c), which was aimed at protecting against liability[.]" H.R. Rep. No. 107-449, at 13 (2002); 28 U.S.C. § 4102(c)(1). As this Court explained in *Roommates.com*, "[t]his express Congressional approval of the courts' interpretation of § 230(c)(1), six years after its enactment, advises us to stay the course of 'robust' webhost immunity." *Roommates.com*, 521 F.3d at 1188.

Internet and to encourage voluntary monitoring for offensive or obscene material.").

Based on its expansive language, and this clear congressional mandate, this Court and others have interpreted Section 230 broadly. *See Carafano*, 339 F.3d at 1123 (collecting cases and explaining that courts across the country "have treated § 230(c) immunity as quite robust" and explained there was a "consensus developing across other courts of appeals that § 230(c) provides broad immunity"). And they have done so even in cases dealing with highly objectionable online content or claims brought by plaintiffs with very sympathetic stories. *See, e.g., Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008); *Klayman v. Zuckerburg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014); *Johnson v. Arden*, 614 F.3d 785, 791-792 (8th Cir. 2010).

These courts were not indifferent to plaintiffs' plights, nor did they approve of the objectionable content at issue. Rather, these cases reflected a broader commitment to "self-regulation, rather than regulation compelled at the sword point of tort liability." *Barrett v. Rosenthal*, 40 Cal. 4th 33, 53 (2006).

C. Holding Intermediaries Liable For Providing Accounts And Messaging Services Would Gut Section 230

Twitter has explained why, as a matter of law, Section 230 applies not just to claims arising from particular pieces of objectionable content, but also to broader publisher activity, including the act of providing

accounts to users who may misuse them and offering a private online messaging service. We will not repeat that discussion, but instead here emphasize that holding Twitter liable on Appellants' theories would be entirely at odds with the policies underlying Section 230. Indeed, it would offer a recipe for evading the statute through artful pleading, a result that courts have consistently rejected. *See, e.g.*, *MySpace*, 528 F.3d at 419-420; *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1102-03 (9th Cir. 2009), *as amended* (Sept. 28, 2009).

As an initial matter, it makes no sense to immunize services providers for actual third-party content—concrete and visible to all—but then hold service providers liable for failing to *forecast* the content a user might ultimately create at the time that user opens an account. Indeed, the First Circuit has held that an online platform's decision "not [to] prevent a single individual from registering under multiple screen names"—an act that allegedly "ma[de] it possible for individuals to spread misinformation more credibly"—was "as much an editorial decision with respect to that misinformation as a decision not to delete a particular posting." *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 416, 420, 422 (1st Cir. 2007).

Appellants try to create an artificial distinction between users and their content—but imposing liability for failing to prevent certain users from accessing online services is just another way of holding Internet service providers liable for third-party content. *See Fields v. Twitter,*

Inc., 217 F. Supp. 3d 1116, 1123 (N.D. Cal. 2016) ("prohibit[ing] ISIS members and affiliates from acquiring accounts . . . [is] a policy that necessarily targets the content, ideas, and affiliations of particular account holders"); *see also Cohen v. Facebook, Inc.*, *Force v. Facebook, Inc.*, No. 16-CV-4453 (NGG) (LB), 2017 WL 2192621, at *12 (E.D.N.Y. May 18, 2017) ("choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform"). Accepting this distinction would nullify Section 230's protection of online services from liability for third-party activity.

It also makes no sense under Section 230 to distinguish between online public content and content in online messaging. As explained in detail above, one of the dual purposes of Section 230 was to encourage robust online communication. Whether that online communication takes the form of a public post or a single message (shared with a smaller set) makes no difference to the congressional goals of "promot[ing] the continued development of the Internet," "preserv[ing] the vibrant and free market that presently exists for the Internet," and "maximize[ing] user control." 47 U.S.C. § 230(b)(1)-(5).

Appellants also imply that Twitter should have known not to provide accounts or messaging to certain users based on the content these users posted on *other* accounts. Given the amount of content posted by third parties on the site, reviewing all potentially-related content would become an impossible task. Imposing liability for failing

to do so would not only bring us back to the *Stratton* regime that Congress explicitly rejected, it may have precisely the opposite effect of what our members want—an Internet that is as safe as it is vibrant.

If Appellants prevail, Internet companies, both large and small, might face the "grim choice"—described by this Court en banc in *Roommates.com.* Forcing that dilemma on companies would run the risk of sabotaging the steps they already take, such as employing teams of human reviewers to analyze reports of offensive and dangerous activity on their systems. No one—not even the most sophisticated law enforcement and intelligence communities in the world—can work with perfect precision. Congress recognized that holding Internet companies liable for all user activity in situations like this might make the perfect the enemy of the good.

III. CONCLUSION

The District Court correctly applied Section 230 to dismiss this case. That ruling should be affirmed.

DATED: June 7, 2017

Respectfully submitted,

/s/ Sonali D. Maitra
SONALI D. MAITRA
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666
smaitra@durietangri.com

Counsel for Amicus Curiae

Internet Association

CERTIFICATE OF COMPLIANCE

I hereby certify that pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1 this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and (6), because it is written in 14-pt Century Schoolbook font, and with the type-volume limitations of Fed. R. App. P. 29(d) and Ninth Circuit Rule 29-2(c), because it contains 3,078 words, excluding the portions excluded under Fed. R. App. P. 32(a)(7)(B)(iii). This count is based on the word count feature of Microsoft Word.

DATED: June 7, 2017

/s/ Sonali D. Maitra

Sonali D. Maitra
DURIE TANGRI LLP
Counsel for Amicus Curiae Internet Association

9th Circuit Case Number(s) 16-17165

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) Jun 7, 2017 .

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Signature (use "s/" format) /s/ Sonali D. Maitra

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)