No. 21-1333

In the
Supreme Court of the United States

REYNALDO GONZALEZ, et al.,
Petitioners,
v.
GOOGLE LLC,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF FOR META PLATFORMS, INC. AS AMICUS CURIAE IN SUPPORT OF RESPONDENT

THEODORE J. BOUTROUS JR.
AMIR C. TAYRANI
RUSSELL B. BALIKIAN
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Ave., NW
Washington, DC 20036

KRISTIN A. LINSLEY
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105

ALLYSON N. HO
BRAD G. HUBBARD
GIBSON, DUNN & CRUTCHER LLP
2001 Ross Ave., Suite 2100
Dallas, TX 75201

EMILY RIFF
GIBSON, DUNN & CRUTCHER LLP
1801 California Street, Suite 4200
Denver, CO 80202

PAUL D. CLEMENT
Counsel of Record
ERIN E. MURPHY
JAMES Y. XI*
CLEMENT & MURPHY, PLLC
706 Duke Street
Alexandria, VA 22314
(202) 742-8900
paul.clement@clementmurphy.com

JENNIFER NEWSTEAD
SCOTT TUCKER
SANDEEP SOLANKI
NATALIE NAUGLE
NIKKI STITT SOKOL
META PLATFORMS, INC.
1601 Willow Road
Menlo Park, CA 94025

*Supervised by principals of the firm who are members of the Virginia bar

Counsel for Meta Platforms, Inc.

January 19, 2023

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 1

ARGUMENT 6

I. Meta Has Robust Policies Prohibiting Terrorist Content And Relies On Algorithms To Enforce Them. 6

A. Meta Is an Industry Leader in Efforts to Keep Terrorists and Terrorist Content Off Its Services 7

B. Algorithms Are a Critical Component of Meta's Anti-terrorism Policies 10

II. Decisions About How To Organize And Display Third-Party Content Fall Within The Heartland Of §230's Protection........................ 16

A. Congress Enacted §230 to Provide Websites with Broad Protection Against Liability for Their Users' Speech 17

B. Section 230 Bars Petitioners' Claims 22

III. Petitioners' Proposal To Protect Removing Content But Not "Recommending" It Would Rewrite The Statute And Create Incentives to Remove Content That Congress Never Intended 28

CONCLUSION 33

TABLE OF AUTHORITIES

Cases

Anderson v. N.Y. Tel. Co.,
345 N.Y.S.2d 740 (1973) 18, 19

Balabanoff v. Fossani,
81 N.Y.S.2d 732 (Sup. Ct. 1948)............................ 18

Citizens United v. FEC,
558 U.S. 310 (2010).. 29

Cubby, Inc. v. CompuServe, Inc.,
776 F.Supp. 135 (S.D.N.Y. 1991) 20

Daniel v. Armslist, LLC,
926 N.W.2d 710 (Wis. 2019) 23

Daniel v. Dow Jones & Co.,
520 N.Y.S.2d 334 (Civ. Ct. 1987)........................... 19

Force v. Facebook, Inc.,
934 F.3d 53 (2d Cir. 2019) 16, 24

Gertz v. Robert Welch, Inc.,
418 U.S. 323 (1974).. 19

Hustler Magazine, Inc. v. Falwell,
485 U.S. 46 (1988).. 30

Nat'l Ass'n of Mfrs. v. Dep't of Def.,
138 S.Ct. 617 (2018)... 26

Nat'l Rev., Inc. v. Mann,
140 S.Ct. 344 (2019).. 30

New York Times v. Sullivan,
376 U.S. 254 (1964).. 19

O'Brien v. W. Union Tel. Co.,
113 F.2d 539 (1st Cir. 1940) 18

Peck v. Tribune Co.,
214 U.S. 185 (1909).. 17

Stratton Oakmont, Inc. v. Prodigy Servs. Co.,
1995 WL 323710
(N.Y. Sup. Ct. May 24, 1995) 20, 21, 25

Zeran v. Am. Online, Inc.,
129 F.3d 327 (4th Cir. 1997) 28

Zeran v. Am. Online, Inc.,
958 F.Supp. 1124 (E.D. Va. 1997) 18

Statutes

47 U.S.C. §230(a) 32

47 U.S.C. §230(b) 32

47 U.S.C. §230(c)(1) 22, 26

47 U.S.C. §230(e)(3) 22

47 U.S.C. §230(f)(4) 25, 26, 27

Other Authorities

Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds: Hearing Before S. Comm. on the Judiciary, Subcomm. on Privacy, Technology & the Law, 116th Cong. (2021),
https://bit.ly/3whTcmM 12, 13, 15

Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, Richmond J. of Law & Technology (Aug. 27, 2020) 16

Dangerous Individuals and Organizations,
Meta, https://bit.ly/3wdslbS
(last visited Jan. 19, 2023) 8

Dangerous Organizations: Terrorism and Organized Hate, Meta, https://bit.ly/3XiHRyQ (last visited Jan. 19, 2023) 15

Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation: Hearing Before the H. Comm. on Homeland Security, 116th Cong. (2019), https://bit.ly/3Xl1kz3 .... 7, 9, 10, 15

How Feed Works, Facebook, https://bit.ly/3QTlkGr (last visited Jan. 19, 2023) 12

R. Hayes Johnson, Jr., *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in* Stratton Oakmont, Inc. v. Prodigy Services Co., 49 Ark. L. Rev. 589 (1996).............................. 20

Mass Violence, Extremism, and Digital Responsibility Before S. Comm. on Commerce, Science & Transp., 116th Cong. (2019), https://bit.ly/3XlkMM3 15

Meta Platforms, Inc., Annual Report (Feb. 3, 2022)... 8

Michael I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" within the New Media*, 71 Notre Dame L. Rev. 79 (1995) 21

New Oxford American Dictionary (3d ed. 2010)... 11

Oxford American Dictionary (1st ed. 1980) 11

Platform Safety, Meta, https://bit.ly/3XX9Jsv (last visited Jan. 19, 2023) 9

Press Release, Meta Platforms, Inc., *Meta Achieves Brand Safety Milestone for Facebook With MRC Accreditation* (Nov. 1, 2022), https://bit.ly/3wed6iQ 9

Restatement (Second) of Torts (1977).......... 17, 18, 19

Terrorism and Social Media: #IsBigTechDoingEnough: Hearing Before the S. Comm. on Commerce, Science, & Transp., 115th Cong. (2018), https://bit.ly/3kvkvru 10

What are Recommendations on Facebook?, Facebook, https://bit.ly/3ZK1S33 (last visited on Jan. 19, 2023) 13

Why do I See Suggested Content in My Facebook Feed?, Facebook, https://bit.ly/3XJy4BT (last visited Jan. 19, 2023) 13

STATEMENT OF INTEREST[1]

Amicus curiae Meta Platforms, Inc. is a technology company, founded in 2004, whose mission is to give people the power to build communities and bring the world closer together. Meta's services include Facebook and Instagram and are used by billions of people worldwide. Meta has a profound interest in this case for at least three reasons. First, Meta is a party in *Twitter, Inc. v. Taamneh*, No. 21-1496, which arises out of the same Ninth Circuit decision under review here and involves materially identical claims. Second, given the scope of its services and its billions of users, Meta has been named as a defendant in countless lawsuits that implicate §230, enacted as part of the Communications Decency Act. Third, like virtually every other service protected by §230, Meta uses algorithms to organize and display tens of millions of pieces of content that users share every day, and to identify and remove the small subset of content that violates its terms and policies, including content supporting terrorism. Meta thus has a strong interest in the proper interpretation of §230 as it relates to those activities.

SUMMARY OF ARGUMENT

This case involves an effort to hold online services liable for "recommending" content and to narrow

[1] Pursuant to Supreme Court Rule 37.6, *amicus curiae* states that no counsel for any party authored this brief in whole or in part and that no entity or person, aside from *amicus curiae*, its members, and its counsel, made any monetary contribution toward the preparation or submission of this brief. Pursuant to Supreme Court Rule 37.3, counsel of record for all parties have consented to this filing in letters on file with the Clerk's office.

§230's protections in a way that would strongly incentivize them to remove even *more* third-party content. Petitioners' effort is deeply flawed as a legal matter, as interpreting §230 to protect removing content but not "recommending" it not only has no grounding in the statutory text, but also ignores the way the internet actually works. And it is misguided as a practical matter, as drawing such a distinction for liability purposes would incentivize online services to remove important, provocative, and controversial content on issues of public concern, frustrating what Congress intended to be a vibrant marketplace of diverse perspectives.

Like most social-media companies, Meta has long had strict policies prohibiting terrorists and terrorist groups, as well as posts that praise or support such individuals and groups, on its services. Those policies help to ensure that Meta's services are places that users want to frequent and advertisers want to advertise. Meta has invested billions of dollars to develop sophisticated safety and security systems that work to identify, block, and remove terrorist content quickly—typically before it is ever seen by any users. In the third quarter of 2022 alone, Meta blocked or removed nearly 17 million pieces of third-party content for violating its terrorism policies, and it identified 99.1 percent of that content on its own. If terrorism-related content evades Meta's first-line defenses, Meta has in place measures to mitigate the risk that it will be shown to others.

Petitioners do not deny that §230 protects online services' decisions to remove terrorist content. But they attempt to divine a sharp distinction between efforts to *remove* third-party content, which they concede §230 fully protects, and decisions to "recommend" third-party content, which they contend §230 does not protect. It is far from clear that this purported distinction would matter in this case, as petitioners have never alleged that any "recommended" content precipitated the horrific attacks of terrorism that caused their injuries. Indeed, there are no allegations that the terrorists who carried out those attacks even viewed social media—much less that they viewed ISIS videos on YouTube because Google "recommended" them. The absence of any such allegations makes this a singularly inappropriate vehicle to draw such a distinction.

But in all events, petitioners' purported recommendation/removal distinction for liability purposes is illusory, as it has no grounding either in the statutory text—which broadly describes the third-party "information" for which an interactive computer service may not be held liable, and nowhere mentions any exception for "recommendations"—or in how websites actually function. Petitioners are not challenging some statement where Google or YouTube affirmatively endorsed the content of a particular video. The "recommendations" they challenge are implicit, based simply on the manner in which YouTube organizes and displays the multitude of third-party content on its site to help users identify content that is of likely interest to them. But it is impossible to operate an online service *without* "recommending" content in that sense, just as it is impossible to edit an anthology without "recommending" the story that comes first in the volume.

Indeed, since the dawn of the internet, virtually every online service—from news, e-commerce, travel, weather, finance, politics, entertainment, cooking, and sports sites, to government, reference, and educational sites, along with search engines—has had to highlight certain content among the thousands or millions of articles, photographs, videos, reviews, or comments it hosts to help users identify what may be most relevant. Given the sheer volume of content on the internet, efforts to organize, rank, and display content in ways that are useful and attractive to users are indispensable. As a result, exposing online services to liability for the "recommendations" inherent in those organizational choices would expose them to liability for third-party content virtually all the time.

That result would be impossible to reconcile with §230's plain text and evident purpose. Whatever else one may say about the scope of §230, there can be no serious dispute that its core protection for online services is against liability for the third-party content that they host, even though they exclude some material *and* organize the material they host to make it useful for users. Indeed, the statute was enacted to counter cases that held online services liable for third-party content they hosted, not for content they removed. Any reading of §230 that would exclude from its protections virtually everything that it was enacted to protect just because material is presented in a format with utility for the user is a complete non-starter.

Seemingly recognizing that problem, the United States tries to draw a distinction between "a website's choices about the organization and presentation of user-generated content," which it agrees §230 protects, and what it labels "targeted recommendations," which it would deem outside the scope of §230. U.S.Br.29-30. But that distinction is illusory. So-called "targeted recommendations" reflect nothing more than how online services organize and display content. They differ from other more static organizational choices only in that they harness the power of the internet to personalize content on a user-by-user basis rather than through a one-size-fits-all approach. There is no coherent basis for depriving an online service of §230's protection for those core publisher functions just because the technological advances Congress wanted to protect enable online services to personalize content so users might see what they actually want.

Petitioners' removal/recommendation dichotomy not only finds no support in the statutory text, but also would create incentives to remove content that challenges the established orthodoxy, which would run directly counter to Congress' efforts in enacting §230. If online services risk substantial liability for disseminating third-party content (or for doing so in useful formats that prioritize information users want to view) but not for removing third-party content, they will inevitably err on the side of removing content that comes anywhere close to the potential liability line. Those incentives will take a particularly heavy toll on content that challenges the consensus or expresses an unpopular viewpoint. After all, the more third-party content challenges the consensus, the greater the liability risk an online service hosting it faces before juries that will likely reflect or at least be influenced by the consensus view. Depriving online services of §230's critical protections when it comes to any content they host in useful formats, but nothing they remove, would create incentives for them to host only uncontroversial content and remove material that deviates from the consensus. The text of §230, which mentions "recommendations" not at all, provides no support for this skewed system. If §230 is truly to be converted into a regime at such profound odds with Congress' express findings and purposes, that decision should come from Congress, not this Court.

ARGUMENT

I. Meta Has Robust Policies Prohibiting Terrorist Content And Relies On Algorithms To Enforce Them.

Meta has adopted terms and policies and exercises editorial discretion to make its services attractive to users and advertisers. As a critical component of that effort, Meta enforces a zero-tolerance policy against the use of its platform by terrorists or terrorist groups, and strictly prohibits any content that supports or praises terrorism. Meta devotes extensive resources to keeping terrorists and terrorist content off its services. Terrorists and terrorist content are aggressively removed, and Meta deploys additional safeguards to mitigate the risk that any forbidden content that does slip through will be shown to others. In short, Meta's consistent policy is that there is no place for terrorism on Facebook or any other Meta service, and its systems rigorously enforce that policy.

A. Meta Is an Industry Leader in Efforts to Keep Terrorists and Terrorist Content Off Its Services.

Meta is committed to making Facebook a safe community for its users to share content, express their opinions, and connect with others. Moreover, its business model depends on making its services attractive to advertisers, whose products are advertised side-by-side with user-generated content. To those ends, Meta leads the industry in identifying and removing terrorism-related content.

Meta has always prioritized the safety of its users. Facebook started as a place for college students to connect and keep up with their friends. Facebook was among the first social-media services to establish and enforce clear content policies designed to foster a safe, secure experience for users. Its anti-terrorism policies date back more than a decade. As Facebook's Vice President for Global Policy Management testified to Congress, "On terrorist content, our view is simple: There is absolutely no place on Facebook for terrorists." *Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation: Hearing Before the H. Comm. on Homeland Security*, 116th Cong., at 6 (2019) (testimony of Monika Bickert, Facebook Vice President for Global Policy Management), https://bit.ly/3Xl1kz3.

That policy is essential both to provide a safe environment for Meta's users and to attract and retain the advertisers that keep Meta's services available to users for free. Advertisers provide "substantially all" of Meta's revenue. Meta Platforms, Inc., Annual

Report 7 (Form 10-K) (Feb. 3, 2022). Just as users do not want to encounter terrorist content when they engage on Facebook, advertisers have made clear that they do not want their advertisements displayed alongside such content. Meta thus must have effective anti-terrorism policies to thrive.

Meta's policies of identifying and removing terrorist content from Facebook are described in its terms of service and content policies, including the "Facebook Community Standards." The policy on "Dangerous Individuals and Organizations" states that Meta "do[es] not allow organizations or individuals that proclaim a violent mission or are engaging in violence to have a presence on Facebook." *Dangerous Individuals and Organizations*, Meta, https://bit.ly/3wdslbS (last visited Jan. 19, 2023). Meta implements that policy through a three-tiered classification system under which terrorists and terrorist organizations—including organizations that, like ISIS, have been designated by the U.S. government as foreign terrorist organizations—are classified as "Tier 1 entities" subject to the most restricted treatment. *Id.* Meta forbids all "praise, substantive support, and representation of Tier 1 entities[,] as well as their leaders, founders, or prominent members." *Id.* Meta also forbids content that praises, supports, or represents terrorist attacks or their perpetrators. *Id.* Those are policies no government could adopt consistent with the First

Amendment, but they are vital to Meta's effort to ensure that its services remain attractive to users.[2]

Meta devotes significant resources to enforcing these policies. Meta has invested billions of dollars and currently has more than 40,000 people worldwide working on its safety and security teams, including those that enforce its anti-terrorism policies. *See Platform Safety*, Meta, https://bit.ly/3XX9Jsv (last visited Jan. 19, 2023). And Meta employs hundreds of highly trained professionals—including counter-terrorism experts and former prosecutors, law-enforcement officials, and intelligence officials—to focus exclusively on preventing terrorist content from appearing on Facebook in the first place and quickly identifying and removing any content that evades first-line protections. *Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation*, *supra*, at 6. These commitments recently led to Meta's accreditation for content-level Brand Safety on Facebook. *See* Press Release, Meta Platforms, Inc., *Meta Achieves Brand Safety Milestone for Facebook With MRC Accreditation* (Nov. 1, 2022), https://bit.ly/3wed6iQ.

Meta's efforts to combat terrorism do not end with policing its own services. Meta also engages with

[2] "Tier 2 entities" are those that engage in violence against state or military actors (rather than civilians). Meta's policy is to remove all support for and representation of Tier 2 entities, their leaders, and their prominent members, as well as any praise for their activities. *Id.* "Tier 3 entities" are those that repeatedly violate Meta's policies or demonstrate a strong intent to engage in violence in the near future. They too are barred from Meta's services. *Id.*

other companies, researchers, and governments to combat terrorism. Meta is a founding member and current chair of the Global Internet Forum to Counter Terrorism, a non-governmental organization dedicated to preventing terrorists from exploiting digital platforms. *Terrorism and Social Media: #IsBigTechDoingEnough: Hearing Before the S. Comm. on Commerce, Science, & Transp.*, 115th Cong., at 7-8 (2018) (testimony of Monika Bickert, Facebook Head of Product Policy and Counterterrorism), https://bit.ly/3kvkvru ("*Terrorism and Social Media*"). Meta led the development of a global database of photographs and videos that companies can use to quickly identify and block or remove terrorist content, as well as a free, open-source software tool that enables companies to "identify copies of images or videos and take action against them en masse." *Id.* at 7-8. And when Meta finds evidence of imminent harm through possible terrorist activities, it promptly informs authorities. *Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation*, *supra*, 6

B. Algorithms Are a Critical Component of Meta's Anti-terrorism Policies.

Keeping terrorism-related content off Meta's services is no mean feat. It depends on the hard work of hundreds of terrorism-focused security experts, and on sophisticated tools Meta has developed, including algorithms and other automated processes. *See Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation*, *supra*, 6. Indeed, algorithms are essential to the orderly functioning of Meta's services and of most sites and services that define the internet. Tens of millions of pieces of third-party content are posted to Meta services every day—far more than even a legion of employees could feasibly manually review. Without algorithms and other automated processes Meta has developed to organize, sort, filter, and, when necessary, block or remove third-party content, Meta could not offer the kind of service its users and advertisers seek, let alone successfully enforce its anti-terrorism policies.

Algorithms are ubiquitous and are hardly a 21st-century phenomenon. Although the term's meaning has evolved, it dates back centuries to a 9th-Century Persian mathematician. In its modern conception, it simply means step-by-step instructions for solving problems or performing tasks. *See New Oxford American Dictionary* 40 (3d ed. 2010) ("algorithm" is a "process or set of rules to be followed in calculations or other problem-solving operations, esp. by a computer"); *accord Oxford American Dictionary* 17 (1st ed. 1980). While the term captures everything from cooking recipes to complex computing programs, algorithms are indispensable when it comes to modern computing applications that require tasks to be automated at scale—so much so that algorithms are part of any introductory computer science course and employing them is a required skill for any entry level software engineer position.

Algorithms are especially useful for managing the massive quantities of information available on the internet and providing users with an organized, easy-to-navigate online experience. Search engines, for example, use algorithms to display websites in order of relevance based on (among other factors) users' search terms and how much traffic each website receives. Legal databases use algorithms to identify potentially relevant cases by comparing the language of a draft brief with the language of judicial opinions. And online-storage websites use algorithms to suggest folders and file names for pictures based on when and where they were taken. In short, algorithms are essential to making the internet function as users expect. Without them, the internet would devolve into a disorganized collection of haphazardly assembled information that would be impossible to navigate.

Meta—like virtually all online services—uses algorithms to ensure that its services function in ways that attract and retain users and advertisers. Facebook's automated systems help users see content shared by friends, family members, and others they choose to follow. Facebook displays a constantly updated "feed" of posts on a homepage personalized for each user, and it uses algorithms to rank and organize the thousands of posts a user is eligible to see at any given moment based on how likely they are to be meaningful to the user.[3] *See generally Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds: Hearing Before S. Comm. on the Judiciary, Subcomm. on Privacy, Technology & the Law*, 116th Cong., at 1-2 (2021) (prepared statement of Monika Bickert, Facebook Vice President for Content Policy), https://bit.ly/3whTcmM.

[3] "Feed is the constantly updating list of stories in the middle of your home page. *See How Feed Works*, Facebook, https://bit.ly/3QTlkGr (last visited Jan. 19, 2023).

For the most part, these algorithms are driven by inputs that come from the user, as the goal is to make it easier for each user to find content the user wants to see. To that end, Facebook's algorithms take thousands of signals generated from a combination of the user's activity and preferences (*e.g.*, friends, groups the user follows, content the user reads) and various characteristics of third-party content (*e.g.*, who posted it, when, what type of content it is) to predict which content a user is likely to find of interest. *Id.* Meta explains to users how its systems work and gives them tools to control what they see in their feeds. For example, Facebook users can opt to prioritize recent-in-time posts or to highlight (or mute) content from specific friends or pages. These user-driven algorithms run every time a user loads or refreshes his or her feed (*i.e.*, hundreds of millions of times a day across Facebook's user base).

Meta's algorithms also help users discover new content that may interest them.[4] For example, someone who is friends with several people who went to high school or college with another person with whom he is not friends might be interested in making a new connection; someone who likes Major League Baseball's Facebook page might be interested in content from the local team's Facebook page; someone

[4] Facebook explains the factors it considers when displaying content (*e.g.*, who interacted with the content, related topics, location); provides people with control over content they see; and discloses its guidelines regarding content it suggests. *See What are Recommendations on Facebook?*, Facebook, https://bit.ly/3ZK1S33 (last visited on Jan. 19, 2023); *Why do I See Suggested Content in My Facebook Feed?*, Facebook, https://bit.ly/3XJy4BT (last visited Jan. 19, 2023).

who follows an up-and-coming politician or artist might be interested in attending a local event at which they are speaking or performing. Countless people have met their spouses, tracked down lost relatives, secured new jobs, taken up new hobbies, donated to new causes, started businesses, found solace with others suffering from similar tragedies, and even established new religious or spiritual movements owing to services like Facebook.

Meta also employs algorithms to deliver advertisements to users, based on a combination of criteria specified by the advertisers and, within those specifications, information about the advertisements and user activity. As with content shared by other users, users may be eligible to see tens of millions of advertisements at any given moment, but only a subset can be delivered to a user's feed. Meta's systems help users connect with the most relevant advertisements, which not only helps enable Meta to provide its services free of charge, but also helps advertisers of all sorts grow and sustain their businesses, audiences, or followings.

Without these and other algorithms, Facebook, and the internet more generally, would be virtually impossible to navigate and much less useful or relevant to the daily lives of hundreds of millions of people. Given the sheer quantity of third-party content posted every day, users would quickly become overwhelmed with mountains of irrelevant content, with no easy way to obtain or discover the information most meaningful to them.

While algorithms are essential to Meta's efforts to organize content Meta welcomes, they are equally vital to Meta's efforts to identify, block, and remove content it categorically forbids, including content promoting terrorism. Indeed, the reason terrorism-related content rarely makes it onto Facebook is because Meta has invested heavily in sophisticated systems that identify, flag, remove, or block the millions of terrorism-related posts it confronts. In the third quarter of 2022, for example, Meta removed nearly 17 million terrorism-related posts—far more than could be caught through manual review. Meta's systems flagged and took down 99.1 percent of those posts without relying on a users to report them. *Dangerous Organizations: Terrorism and Organized Hate*, Meta, https://bit.ly/3XiHRyQ (last visited Jan. 19, 2023).

For example, Meta's algorithms can screen text for terrorism-related content and match newly posted images and videos with known terrorist content and block them before they are displayed. *Examining Social Media Companies' Efforts to Counter On-Line Terror Content and Misinformation*, *supra*, 8. And Meta complements those automated processes with extensive human review and tools for users to flag any terrorist content. *See Mass Violence, Extremism, and Digital Responsibility Before S. Comm. on Commerce, Science & Transp.*, 116th Cong., at 4 (2019) (prepared statement of Monika Bickert, Facebook Vice President for Global Policy Management and Counterterrorism), https://bit.ly/3XlkMM3. Blocked or removed posts, of course, cannot be displayed in any user's feed. *See Algorithms and Amplification*, *supra*, 4 ("If content is removed for violating our Community Standards, it does not appear in News Feed at all."). If any such content evades Meta's robust first-line defenses, Meta has measures to mitigate the risk that it will show up in users' feeds.

It therefore simply is not the case that Meta "unleashes its algorithms" to recommend terrorist content or to connect people based on a shared interest in terrorism. *Force v. Facebook, Inc.*, 934 F.3d 53, 77 (2d Cir. 2019) (Katzmann, J., concurring in part and dissenting in part). To the contrary, Meta employs algorithms and other measures to block or remove most such content before anyone ever sees it. Meta can enforce its anti-terrorism policies so vigorously precisely because of the sophisticated algorithms it has developed.

II. Decisions About How To Organize And Display Third-Party Content Fall Within The Heartland Of §230's Protection.

Petitioners do not take issue with efforts of Meta and other services to use algorithms and other automated processes to *remove* terrorism-related content. To the contrary, petitioners laud those efforts, and appear to agree that §230 protects *all* decisions to remove third-party content.[5] Indeed, petitioners have even filed an amicus brief in *Moody v. NetChoice LLC*, No. 22-277, arguing that it is "highly likely" that §230 preempts various aspects of Florida's effort to override certain websites' editorial judgments in removing or deprioritizing third-party content. Gonzalez.Br.11.

[5] That concession is correct. *See, e.g.*, Christopher Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, Richmond J. of Law & Technology (Aug. 27, 2020).

Petitioners instead rest their theory of §230 liability on a dichotomy between *removing* third-party content (which they view as laudable and protected by §230) and "recommending" third-party content (which they view as falling outside §230). Drawing such a distinction for liability purposes finds no support in the statute and would gut the core protections Congress enacted §230 to provide.

A. Congress Enacted §230 to Provide Websites with Broad Protection Against Liability for Their Users' Speech.

Section 230 was enacted in response to the challenges that had arose from trying to apply a legal regime developed around more conventional forms of communication to the internet and its veritable flood of user-generated content.

At common law, a publisher could be held liable for any harmful content it published, regardless of whether that content contained third-party speech, and someone who re-published that content could be "subject to liability as if he had originally published it." Restatement (Second) of Torts §578 (1977); *id.* cmt. b; *see also Peck v. Tribune Co.*, 214 U.S. 185, 189 (1909).

While virtually anyone who disseminated speech was originally treated as a publisher, many courts walked that rule back over time. For example, courts concluded that those who merely distribute third-party content (*e.g.*, a newsstand or bookstore) could not be subject to liability as the publisher of that content unless they knew or had reason to know its substance. Restatement (Second) of Torts §581 (1977); *id.* cmt. b; *see also Zeran v. Am. Online, Inc.*, 958

F.Supp. 1124, 1133 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).

When telegraph technology came along, courts held that telegraph operators were liabile for the content of an author or speaker only "in the necessarily rare cases where the transmitting agent of the telegraph company happened to know that the message was spurious or that the sender was acting … in bad faith and for the purposes of ... another." *O'Brien v. W. Union Tel.*, 113 F.2d 539, 542-43 (1st Cir. 1940). Although telegraph companies technically published senders' messages, their limited role in assessing and editing those messages, combined with the sheer number of messages sent (200 million annually in 1939), weighed heavily against subjecting them to liability for that third-party content absent knowledge of what it contained. *Id.*

Courts also concluded that mere conduits that simply provide equipment or facilities used for general communication purposes (*e.g.*, telephone companies) were immune from liability for the speech of those who use their equipment or facilities. *See* Restatement (Second) of Torts §581 (1977). For example, telephone companies were completely immune from liability for third-party content even if they knew "about the nature of the message being communicated." *Anderson v. N.Y. Tel.*, 345 N.Y.S.2d 740, 752 (1973) (Witmer, J., dissenting), *dissent adopted by* 320 N.E.2d 647 (N.Y. 1974). Given that they play no role "in preparing the message" and have no "discretion or control over its communication," courts concluded that their role is "not legally different" from that of "a person who leases a sound amplification system to a person who makes a defamatory public speech, or who leases a typewriter to one who writes defamatory messages or a tape recorder to one who broadcasts a defamatory message." *Id.*

Radio and television broadcasters, by contrast, were generally treated as publishers. Although many stations leased airtime to third parties, courts held that they were "more nearly analogous to a newspaper or the publisher of a book than to a telegraph company" because broadcasters "select and put upon the air their own programs" and "cooperate actively in the publication" of others' programs. Restatement (Second) of Torts §581, cmt. g (1977). That said, the largely judge-made rules governing liability for publishing third-party content relaxed considerably over time. Strict liability for third-party content can no longer attach regardless of whether one publishes the content or distributes it. Publishers instead typically must (at least) have knowledge of the substance of the wrongful content. *See*, *e.g.*, *Gertz v. Robert Welch*, 418 U.S. 323, 347-50 (1974); *New York Times v. Sullivan,* 376 U.S. 254, 279-80 (1964).

Applying these rules to the internet proved very complicated when state and federal courts confronted that new technology. Some of the earliest internet cases were relatively straightforward. For example, a New York state court had little trouble concluding that a company that made its own news reports available online for $3.00 per minute should be treated like a publisher. *Daniel v. Dow Jones & Co.*, 520 N.Y.S.2d 334, 340 (Civ. Ct. 1987). But the traditional modes of analysis were complicated by the fact that, "unlike any traditional form of information publishing or distribution, computer communication is a self-actuating process"—*i.e.*, "most information is generated by individuals sitting in the privacy of their homes." R. Hayes Johnson, *Defamation in Cyberspace: A Court Takes a Wrong Turn on the Information Superhighway in* Stratton Oakmont, Inc. v. Prodigy Services Co., 49 Ark. L. Rev. 589, 620 (1996). Thus, when it comes to content created and posted on a website by a third party, the internet combines publishing, distributing, and providing a conduit for communication in one single service.

In one of the earliest cases involving liability for third-party content, a New York federal court held that a website could be held liable for third-party content only if "it knew or had reason to know of the allegedly [harmful] statements." *Cubby, Inc. v. CompuServe, Inc.*, 776 F.Supp. 135, 139-41 (S.D.N.Y. 1991). The court reached that conclusion principally because CompuServe had "little or no editorial control over [its website's] contents," and instead contracted with a third party to "manage, review, create, delete, edit and otherwise control the contents" of its electronic bulletin boards. *Id.* at 137, 140. Reasoning that CompuServe was effectively "a news distributor," the court granted it summary judgment because there was no evidence that it "knew or had reason to know of [its website's] contents." *Id.* at 141.

A few years later, a New York state court reached a very different conclusion in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). Unlike CompuServe, which did not screen or filter third-party content on its website, Prodigy marketed itself as a "'family-oriented' computer service." *Id.* at *5. To that end, Prodigy established "content guidelines" and used an "automatic software screening program" (*i.e.*, an algorithm) to identify, block, and delete posts that violated them. *Id.* at *2-5. The court held that Prodigy should be treated as a publisher—*i.e.*, liable for all third-party content on its website—because Prodigy exercised editorial control by "actively utilizing technology and manpower to delete" third-party posts, thereby determining "what is proper for its members to post and read." *Id.* at *4.

The *CompuServe* decision had already faced considerable criticism, as its knowledge-based regime was highly impractical vis-à-vis the internet and created incentives to turn a blind eye to harmful content. *See, e.g.*, Michael Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" within the New Media*, 71 Notre Dame L. Rev. 79, 120 & n.273 (1995). But the *Prodigy* decision made matters far worse, as it created a regime under which a website exercising *any* discretion to remove harmful or offensive third-party content would risk being treated as the publisher of—and thus liable for all third-party content on its site. As Congress quickly recognized, such a rule would create perverse incentives by penalizing websites for trying to protect users from things like obscenity or content promoting terrorism or inciting violence. Congress thus took swift action to course-correct.

To that end, Congress enacted §230, which eliminates liability for third-party content altogether for websites that host it: "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). Given the national—indeed, global—scope of the internet, Congress did not leave matters to the judges of 50 different states trying to adopt common-law rules to the emerging internet. It expressly preempted inconsistent state and local law. *See* 47 U.S.C. §230(e)(3) ("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."). In effect, §230(c)(1) overruled both *Prodigy* and *CompuServe*, declaring that an interactive computer service provider cannot be held liable as a publisher of third-party content, period, regardless of whether it is more akin to a publisher or distributor.

For good measure, §230(c)(2) confirms that online services cannot be held liable based on efforts to block, remove, or restrict access to third-party content. Section 230(c)(2)'s protections are in addition to those provided by §230(c)(1), which bars all claims that seek to treat an online service as a publisher or speaker of third-party content—regardless of any action it took (or did not take) regarding that content. That is, Congress made clear that §230 does not obligate an online service to carry any particular content or impose liability for declining to do so.

Section 230 thus provides broad and comprehensive protection against efforts to hold online services liable for the speech of their users.

B. Section 230 Bars Petitioners' Claims.

Section 230 bars any effort to treat an online service as the publisher or speaker of information provided by a third-party content provider. That is exactly what petitioners seek to do. Petitioners try to frame this case as something else, focusing on content supposedly created by Google when it supplies users with links to third-party content on YouTube. Gonzalez.Br.14, 33-40. But this case is not about the random string of letters, numbers, and characters that identify where on the internet a YouTube video can be found. It is about the video a user finds if it clicks on that link, as petitioners themselves recognized in their complaint. *See, e.g.*, JA156-63. While petitioners now seek to focus on Google's "recommendations" in isolation from the actual videos allegedly recommended, that is artificial in the extreme. And §230 bars plaintiffs "from using 'artful pleading' to state their claims only in terms of the interactive computer service provider's own actions, when the underlying basis for liability is unlawful third-party content published by the defendant." *Daniel v. Armslist, LLC*, 926 N.W.2d 710, 724 (Wis. 2019).

In all events, shifting the focus to Google's own actions does not help petitioners' cause, as they fail to identify any action taken by Google that is not protected by §230. According to petitioners, by using algorithms to identify and facilitate access to third-party content that a user is likely to find of interest, Google engages in its own speech of "recommending" content, and hence is no longer protected by §230.

As an initial matter, that theory struggles to find footing in petitioners' allegations. Although petitioners allege that YouTube helped broaden ISIS's influence, they do not allege that the terrorists who carried out the attacks viewed any content on YouTube—much less viewed ISIS-related content after and because they received a "targeted recommendation" or YouTube-generated link. At any rate, petitioners' argument is irreconcilable with §230. What they mean by "recommendations" are just Google's efforts to organize and display third-party content to make it accessible to a broader public—conduct that not only is at the heart of publishing, but is unavoidable for online services given the way the internet works. Petitioners thus propose an exception that would gut §230's no-publisher-liability rule.

The sheer amount of third-party content on the internet leaves online services with no choice but to make decisions about how to organize and display content in ways that are useful and attractive to users. Indeed, "since the early days of the Internet," services have "always decided … where on their sites (or other digital property) particular third-party content should reside and to whom it should be shown." *Force*, 934 F.3d at 66. Decisions about how to organize and display content inevitably require judgments not only about what third-party content to display and not display, but about what third-party content to prioritize and deprioritize. Moreover, the whole point of those decisions is to make third-party content more accessible to the intended audience—*i.e.*, to publish the material more effectively. As a practical matter, then, treating those judgments as sufficient to expose a service to liability for "recommending" third-party content would leave it exposed to liability for virtually all the content it makes available to the public, which is exactly what §230 was enacted to prevent.

That YouTube, like virtually all online services of any size, uses algorithms to help carry out those core publishing functions is a practical necessity that does not change the legal analysis in the slightest. Content-recommendation algorithms, like the many other algorithms online services use to curate, block, and display third-party content, are just a way of "organiz[ing] and present[ing] … user-generated content." U.S.Br.29. In *Prodigy*, Prodigy explained that "its automatic software screening program" played a critical role in enabling it "to regulate the content of its bulletin boards." *Stratton Oakmont*, 1995 WL 323710, at *4. There is no coherent reason for treating a service that uses algorithms to filter, sort, and organize "information provided by another information content provider" differently from one that chooses to perform those tasks manually. U.S.Br.30.

The United States correctly acknowledges that "a website's choices about the organization and presentation of user-generated content do not constitute the 'creation or development' of that material." U.S.Br.29. And it agrees that "actions a website takes to better display preexisting third-party content or make it more usable"—including by "pick[ing], choos[ing]," "display[ing]," and "organiz[ing]" content—are covered by the plain text of §230. *See* U.S.Br.22-23 (citing 47 U.S.C. §230(f)(4)). But the United States tries to draw a distinction between the "basic organizational or display tools" that it acknowledges are "inherent in an interactive online service," U.S.Br.23, and so-called "targeted recommendations," which it claims go beyond "pick[ing]," "choos[ing]," and "display[ing]" content and "communicate a message … that is distinct from the messages conveyed by the" third-party content itself. U.S.Br.27 (quoting 47 U.S.C. §230(f)(4)).

That distinction finds no support in the text of §230 or in how "recommendation" algorithms actually work. As best as one can tell, what the United States seems to think differentiates a "targeted recommendation" from other organizational decisions it would protect is that the organization of third-party content is user-specific. But nothing in §230 purports to make its protections turn on whether a service selects one uniform organization for publishing third-party content or chooses to publish it differently depending on the user. The statute prohibits treating an online service "as the publisher or speaker of any information provided by another information content provider," full stop. 47 U.S.C. §230(c)(1). And what matters are "the words that Congress wrote"—"this Court is not free to 'rewrite the statute' to the Government's liking." *Nat'l Ass'n of Mfrs. v. Dep't of Def.*, 138 S.Ct. 617, 629 (2018).

Nor does the United States' proffered distinction make any practical sense. Any decision an online service makes regarding how to sort, pick, organize, and display third-party content conveys an implicit recommendation about that content. That is true for even the simplest methods of organization. Reverse chronological order implicitly recommends that users pay more attention to recent content than older posts. Organizing content based on how many other users have viewed it implicitly suggests that users should care more about what other people find interesting. Organizational decisions do not convey any more or less of a message just because a service chooses to organize content on a more dynamic user-specific basis rather than employing a static one-size-fits-all approach. If anything, organizing content in a dynamic fashion based on each user's preferences conveys *less* of a message from the online service than organizing material based on its own views about what content users should view. The United States thus fails to identify any coherent explanation for its illogical claim that YouTube's "Up Next" feature conveys a message that is not protected by §230 but the myriad other choices online services make about how to display and organize content are protected.

At bottom, "recommending" content is inherent in hosting and displaying third-party content. The "recommendation" algorithms at issue here do not merely "operate in conjunction with YouTube's display of third-party content," U.S.Br.28—they control how that content is displayed. If displaying content based on when it was posted is protected by §230, then so is displaying it based on a series of computations designed to identify what each user likely wants to see. Indeed, there is not the slightest indication in the text of §230 that it was designed to straightjacket websites into a single, uniform organization. Treating decisions that an online service inevitably must make about how best to "pick" and "display" content, 47 U.S.C. §230(f)(4), as a back-door basis to hold them liable for third-party content would render §230 not just "a dead letter," U.S.Br.23, but nonsensical.

III. Petitioners' Proposal To Protect Removing Content But Not "Recommending" It Would Rewrite The Statute And Create Incentives to Remove Content That Congress Never Intended.

Construing §230 to protect efforts to *remove* content but not to "recommend" it, as petitioners propose, not only would be atextual and ahistorical; it would create incentives that would lead services to err on the side of removing content in ways Congress never intended. It would convert §230 from a broad protection designed to encourage online services to remove harmful material, enable people to communicate and share, and foster creativity and innovation, into a regulatory provision that would incentivize online services to remove or restrict a wide swath of expression in an effort to minimize costly litigation and unlimited liability for third-party content.

If online services risk liability for disseminating content but not for removing it, the only rational reaction is to err on the side of removal. *See Zeran v. Am. Online*, 129 F.3d 327, 333 (4th Cir. 1997) (providers have a "natural incentive" to "remove messages" if they are "subject to liability only for the publication of information, and not for its removal"). A regime that exposes services to substantial liability for any third-party content they "recommend" (even by simply making it more accessible to users who have found similar or related material interesting), but insulates them from liability for any controversial matter they remove, would leave them with little practical alternative but to remove more content, not less.

That is particularly true given that §230 says not a word about "recommendations," leaving services unclear which of their inevitable organizational choices will subject them to liability. *See Citizens United v. FEC*, 558 U.S. 310, 324 (2010) ("Prolix laws chill speech for the same reason that vague laws chill speech: People 'of common intelligence must necessarily guess at [the law's] meaning and differ as to its application.'"). If merely displaying third-party content in a user's feed qualifies as "recommending" it, *e.g.*, U.S.Br.27-28, then many services will face potential liability for virtually all the third-party content they host because nearly all decisions about how to sort, pick, organize, and display third-party content could be construed as "recommending" that content. Moreover, if §230 provides no clear guidance about how much organization or customization constitutes a targeted "recommendation"—and it is hard to see how a statute that says nothing about recommendations, let alone targeted ones, could provide clear guidance—yet provides clear and categorical immunity for removing material, the incentive to remove additional material will be unmistakable.

Making matters worse, such a regime would create a natural incentive to remove any third-party content that challenges the existing orthodoxy. Speech that is particularly vital to the robust and uninhibited debate that the First Amendment is designed to foster would almost always be the loser in such a regime. After all, there is little risk of liability for "recommending" content that toes the mainstream line, as that content will already be pervasive. There is little risk of liability for merely repeating the conventional wisdom. Content that expresses heterodox views, by contrast, is much more likely to trigger costly litigation, especially if it turns out to be mistaken with the benefit of hindsight, as plaintiffs will point to the very fact that other services did not display such content in challenging the defendant's decision not to follow suit.

That is especially so when it comes to controversial subjects, as that is the context in which some will use any tool at their disposal, including litigation, to try to silence those with whom they disagree. *See Nat'l Review v. Mann*, 140 S.Ct. 344 (2019) (Alito, J., dissenting from denial of certiorari). Under the regime favored by petitioner and the government, online services that allow controversial material to be re-posted would face potential liability, while services that removed the material would be protected by §230. Artificially constraining §230 thus would ultimately undermine "the free flow of ideas and opinions on matters of public interest and concern." *Hustler Magazine v. Falwell*, 485 U.S. 46, 50-52 (1988).

That artificial line would also greatly reduce incentives to provide useful and innovative services. Billions of people across the world use the internet to search for information, read news, connect with friends, be entertained, and more. The internet is useful for all of those things because online services devote significant time and resources to organizing, presenting, and sorting the vast amount of information that people share and compete for users based on the usefulness of their offerings. Facebook is useful for sharing and finding new ideas and engaging with others in large part because it has committed extraordinary resources to organizing the vast amount of information created by its users and presenting it in a way that facilitates meaningful connections and discovery. Google is useful for finding information because it invested heavily in innovative technology to assess and present users with results it has determined most relevant to the search.

Those services would not be nearly as useful (or as attractive to potential advertisers) if they simply displayed content randomly or chronologically or alphabetically, or they ignored their users' preferences when making organizational decisions. Indeed, one of the strongest preferences users have demonstrated as the internet has evolved is for websites that cater to each individual user's interests in how they organize and display third-party content. The market has responded by offering users more opportunities to discover entertaining and useful content created by people they may not know or might not ever find on their own. And as technology continues to evolve, §230 has allowed websites to provide those in-demand services without undue fear of liability. Exposing websites to liability for responding to user demand would chill innovative services—especially if liability turned, as the United States seemingly would have it, on whether a website chooses to try to create the best experience for each user rather than just employing a one-size-fits-all organizational approach.

None of that is remotely consistent with the findings and policies that Congress embraced in §230. In §230, Congress declared that a "vibrant and competitive free market" of different providers, each exercising discretion to establish standards suited to its online community, is the best path to ensuring that the internet remains "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." 47 U.S.C. §§230(a), (b). And recognizing that even by 1996 the internet had already "flourished, to the benefit of all Americans, with a minimum of government regulation," Congress declared it "the policy of the United States" that the internet should be "unfettered by Federal or State regulation." *Id.* §230(b).

Stripping services of protection based on the organizational decisions inherent in operating online websites, and exposing them to the specter of crippling liability for wide swaths of what they do, threatens to stifle the free expression of ideas and the creation of innovative and diverse services. And it would encourage websites to remove all but the most benign views, turning a marketplace of diverse perspectives into a platform for orthodox perspectives. Particularly given that such a regime would run directly counter to Congress' express findings and purposes in §230, whether to impose it should be a decision for Congress, not this Court.

CONCLUSION

For the foregoing reasons, the Court should affirm.

Respectfully submitted,

THEODORE J. BOUTROUS JR.
AMIR C. TAYRANI
RUSSELL B. BALIKIAN
GIBSON, DUNN
 & CRUTCHER LLP
1050 Connecticut Ave., NW
Washington, DC 20036

KRISTIN A. LINSLEY
GIBSON, DUNN
 & CRUTCHER LLP
555 Mission Street
 Suite 3000
San Francisco, CA 94105

ALLYSON N. HO
BRAD G. HUBBARD
GIBSON, DUNN
 & CRUTCHER LLP
2001 Ross Ave., Suite 2100
Dallas, TX 75201

EMILY RIFF
GIBSON, DUNN
 & CRUTCHER LLP
1801 California Street
 Suite 4200
Denver, CO 80202

PAUL D. CLEMENT
 Counsel of Record
ERIN E. MURPHY
JAMES Y. XI*
CLEMENT & MURPHY, PLLC
706 Duke Street
Alexandria, VA 22314
(202) 742-8900
paul.clement@clementmurphy.com

JENNIFER NEWSTEAD
SCOTT TUCKER
SANDEEP SOLANKI
NATALIE NAUGLE
NIKKI STITT SOKOL
META PLATFORMS, INC.
1601 Willow Road
Menlo Park, CA 94025

*Supervised by principals of the firm who are members of the Virginia bar

Counsel for Meta Platforms, Inc.

January 19, 2023