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 OF NATIONAL SECURITY EXPERTS AS *AMICI CURIAE* IN SUPPORT OF AFFIRMANCE

Christopher J. Wright
Counsel of Record
Adrienne E. Fowler
John R. Grimm
HWG LLP
1919 M St NW #800
Washington, DC 20036
(202) 730-1325
cwright@hwglaw.com
Counsel for Amici Curiae

JANUARY 19, 2023

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATUTORY PROVISION INVOLVED

Section 230 of the Communications Act, 47 U.S.C. § 230, provides, in pertinent part:

* * * * *

(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).

* * * * *

(f) Definitions

As used in this section:

* * * * *

(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.

* * * * *

(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.

INTEREST OF *AMICI CURIAE*[1]

Amici are a bipartisan group of national security experts, each of whom served in important roles in the federal government. *Amici* include, but are not limited to, a former: Director of National Intelligence, Acting and Deputy Director of the Defense Intelligence Agency, Commander of U.S. and International Security Assistance Forces for Afghanistan and Commander of the Joint Special Operations, Acting Administrator of the National Telecommunications and Information Administration and Technology Policy Advisor for the House Permanent Select Committee on Intelligence, Director of the National Geospatial-Intelligence Agency, Director of the Joint Artificial Intelligence Center, Deputy Chief of Staff of the Army, and Special Envoy/Coordinator at the U.S. State Department's Global Engagement Center. *Amici* have developed and implemented our national security strategy and confronted threats from our Nation's geopolitical adversaries. A complete list of *Amici* is included in the appendix.

Foreign adversaries, such as the People's Republic of China, Russia, and Iran, regularly conduct disinformation campaigns on online platforms targeting the United States and its allies. Dangerous and radical non-state actors, such as ISIS and Al

---

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *Amici* or their counsel made a monetary contribution to its preparation or submission.

Qaeda, also use online platforms to spread propaganda and recruit members. Both types of campaigns present serious threats to U.S. national security.

Online platform operators have played and must continue to play an important role in countering the online disinformation and recruitment campaigns. They have the technical expertise to combat our adversaries' efforts and have broad latitude to control content on their platforms, at least under the current understanding of Section 230. In contrast, under our laudable free speech protections, government actors have more limited capabilities with respect to removing and otherwise countering online disinformation and propaganda.

Over the past decade, online platform operators have taken significant steps to counter the efforts of hostile foreign governments and terrorist groups. These efforts include removing disinformation and propaganda, "downranking" such material, and promoting information to counter the disinformation and propaganda.

It is vitally important to our national security that online platform operators continue to counter disinformation and propaganda from hostile foreign governments and terrorist groups. While construing Section 230 and resolving this case, the Court should keep in mind that online platform operators play this critical role and ensure that they have the latitude to continue to do so.

INTRODUCTION AND SUMMARY OF ARGUMENT

Information warfare is nothing new. But the rise of social media and other online platforms has created a new and more treacherous battlefield in the war, where our foreign adversaries can spread disinformation, propaganda, and recruitment materials more widely and more efficiently than ever. Our nation's security requires online platform providers to seek out dangerous foreign adversary content and to take it down or take other measures to stop its spread. Upholding the judgment below would encourage online platform providers to continue to aggressively combat foreign adversary information. In contrast, overturning the judgment below would tilt the battlefield in our foreign adversaries' favor. Such a decision would create an environment where online content providers would need to be cautious about removing or downranking objectionable and dangerous content and would be discouraged from developing advanced methods of identifying such content.

Petitioners and another group of former national security officials (*amici* "Former National Security Officials") focus their arguments on algorithms and contend that the use of algorithms to promote content should open online platform providers to liability. But eliminating Section 230 protection when providers use algorithms and other advanced tools to elevate or curate recommendations directly threatens the entire ecosystem that leading service providers have used to combat threats to national security. Instead, the best way to advance national security is to continue to

shield online platform operators from liability with respect to third-party material, including when a platform algorithmically creates and displays a list of third-party content that may be of interest to a particular end user.

Even if Petitioners' apparent (and unreasonable) belief that we can return to a world where algorithms do not play an important role in helping to curate online platforms were true, such a world would not be better for our national security. Given the enormous quantity of material posted online, online platform operators must rely in part on algorithms to identify and filter out or minimize dangerous material. And such beneficial algorithms are just the flip side of the coin of the algorithms used to promote, suggest, or recommend good content. Maintaining Section 230(c)(1) immunity will encourage operators to continue to develop sophisticated algorithms that will identify both content of interest to users and objectionable content that should be removed or downranked.

The change advocated by Petitioners—eliminating Section 230 protection when online platform providers use algorithms to suggest content—will discourage operators from monitoring and removing dangerous material. That is because if Section 230 is construed to allow Petitioners' suit to go forward, a platform operator could best ensure that it will not be subject to suit by adopting a hands-off approach to dangerous third-party content on the platform.

This may sound counterintuitive. After all, it is common ground that operators are protected from liability by Section 230 when they merely remove

objectionable material. But there is no such thing as neutrally eliminating *just* the bad online content; any step taken to address a particular video or post inevitably increases the relative predominance of the posts that remain, including in lists of recommended content. Since removing or downranking content cannot be separated from "promoting" other content, Section 230 immunity encourages providers to act decisively to stem the spread of dangerous content.

As shown below, online platform operators have taken many useful steps to identify and remove dangerous material. They have not developed perfect methods for doing so and never will. But protecting operators from liability only when they adopt a hands-off approach would, in our view, embolden our foreign adversaries and threaten our national security.

ARGUMENT

Petitioners and the Former National Security Officials who filed as *amici* identify a real problem. The national-security threat posed by hostile foreign and terrorist content online, including disinformation, propaganda, and recruitment media, is genuine and serious. Petitioners and their *amici* also accurately point out that automated algorithms play a large role in sorting and ordering content users can access. But, while we agree entirely with the need to effectively combat harmful foreign influence online, we disagree with Petitioners' proposed solution. A holding that online platform providers lose Section 230 immunity when they use algorithms to organize and present lists of content would, perversely, turn an effective tool for *removing* dangerous content into a potential source of liability.

I. OUR COUNTRY CANNOT EFFECTIVELY COMBAT ONLINE THREATS WITHOUT ONLINE PLATFORMS' PARTICIPATION.

A. Materials Posted by Hostile Foreign Governments and Terrorists Pose a Significant National Security Threat.

There is no question that the modern Internet is a powerful tool for hostile foreign powers, terrorist groups, and quasi-state actors. Foreign states increasingly use social media as a tool to "reach U.S. audiences directly" and manipulate discourse, attack their rivals, and undermine U.S. policy. Nat'l Intel. Council, ICA 2020-00078D, Foreign Threats to the 2020 US Federal Elections (Mar. 10, 2021) (as declassified). They perceive their disinformation operations as a way to undermine the United States while remaining short of the threshold of what is defined as "war." As one scholar put it:

> From public health conspiracies to disinformation about politics, social media has increasingly become a medium for use by states to meddle in the affairs of others[.] . . . From China's disinformation campaigns that painted Hong Kong democracy protestors as violent and unpopular dissidents . . . to Iranian-backed disinformation campaigns targeting political rivals in the Gulf[,] . . . state actors are turning to social media as a tool of geopolitical influence.

Samantha Bradshaw, *Influence Operations & Disinformation on Social Media*, Centre for International Governance Innovation (Nov. 23, 2020),

https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/. Others have made the similar observation that "[t]he Russian government . . . manipulates the information ecosystem to attempt to influence American public opinion and undermine U.S. foreign and domestic policy." *Foreign Influence Operations and Their Use of Social Media Platforms: Hearing Before the S. Select Comm. on Intel.,* 115th Cong. 2 (2018) (Questions for the Record of Laura M. Rosenberger).

B. The Participation of Online Platforms Is Essential to Fighting that Threat.

No matter how sophisticated our national security apparatus, the U.S. government cannot by itself fight the threat that foreign powers and terrorist groups pose. In our extensive professional experience, online platforms' full participation in content removal and moderation efforts is essential. "Both the American public and the U.S. government" share this understanding and "consider major social media companies not as auxiliary actors in online counterterrorism, but as the primary entities responsible for countering terrorist content online." Bennett Clifford, *Online Terrorist Content Removal Policy in the United States*, George Washington University Program on Extremism, Dec. 2021, at 9.

Simply put, online platforms are, inevitably, "more adept and more knowledgeable than the government in managing content on their own platforms." *Id.* Moreover, because the online presence of terrorist groups is "a transnational problem, not subject to the jurisdiction of any single government," *id.*, online platforms do not face the same jurisdictional hurdles

as governments in combatting online terrorists. As a result, "the U.S. government has deferred responsibility to regulate terrorist content online to major social media companies." *Id.*

In addition, online platform operators have more flexibility than the U.S. government to remove content. The First Amendment prevents government actors from penalizing objectionable speech unless it is "directed to inciting or producing imminent lawless action" and "likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969); *see also Schenck v. United States*, 249 U.S. 47, 52 (1919) (articulating the "clear and present danger" test). Private actors, in contrast, may remove content from their online platforms if they find it "objectionable," as Section 230(c)(2) recognizes. Thus, our Constitution, unlike the governing law of our foreign adversaries, rightly prohibits government actors from suppressing material that is merely objectionable. But our laws and traditions allow private publishers to determine what they deem objectionable, and Section 230, as interpreted by the lower courts, protects online platform providers from liability as long as they act in good faith.

Addressing lawful but "merely" objectionable foreign adversary content is especially important to our national security. The most effective disinformation campaigns often contain an element of truth, and "[s]ome of the most vicious and effective active measures in the history of covert action were designed to deliver entirely accurate information." Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* 10 (2020).

Therefore, it is both consistent with our laws and traditions and desirable in light of the threat posed by hostile foreign governments and terrorists to ensure that online platform operators will not face lawsuits when they remove material they consider to be objectionable, even if it is not likely to produce imminent lawless action.

Naturally, online platform providers have not eliminated all objectionable material from their platforms, and never will. But the Court should not overlook their many successes. For example, from July to September 2022, Google terminated over ten thousand YouTube channels linked to "coordinated influence operations" by the People's Republic of China that displayed content criticizing the U.S. semiconductor industry and U.S. sanctions of Chinese tech companies. Shane Huntley, *TAG Bulletin: Q3 2022*, Google Threat Analysis Group (Oct. 26, 2022), https://blog.google/threat-analysis-group/tag-bulletin-q3-2022/ ("*TAG Bulletin: Q3 2022*"). Additionally, when a user searches for terrorism or violent extremism-related content on Facebook, Facebook guides users to resources to help abandon this mindset. *See* Facebook, *Counterspeech*, https://counterspeech.fb.com/en/initiatives/redirect/ (last visited Dec. 26, 2022). Such substantial successes result from significant financial and technological investments. Meta, *Our Progress Addressing Challenges and Innovating Responsibly* (Sept. 21, 2021), https://about.fb.com/news/2021/09/our-progress-addressing-challenges-and-innovating-respons ibly/ (demonstrating that the company invested more than $13 billion in countering

disinformation and terrorist content on the Facebook platform between 2016 and 2021).

Online platforms providers' response to Russian misinformation surrounding its invasion of Ukraine illustrates how these successes make the internet a safer place. Search engine DuckDuckGo reacted by "downranking" websites associated with Russian disinformation in search results, making them less likely to appear in responses to user searches. Twitter, *Post of Gabriel Weinberg, CEO & Founder, DuckDuckGo* (Mar. 9, 2022), https://twitter.com/yegg/status/1501716484761997318. YouTube algorithms also downrank "borderline" content. The YouTube Team, *The Four Rs of Responsibility, Part 2: Raising authoritative content and reducing borderline content and harmful misinformation*, YouTube Official Blog (Dec. 3, 2019), https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-raise-and-reduce/. This policy limits recommendations to Russia-linked channels, even if their content does not squarely violate YouTube terms. *See, e.g.*, *TAG Bulletin: Q3 2022*. Similarly, Meta downranks posts shared by groups and websites that post misinformation or fake links. Since the Russian invasion, Meta has taken further action to demote Russian state-run content, resulting in a "significant reduction" of total engagement on that content. Emmanuel M. Vincent et al., *Measuring the effect of Facebook's downranking interventions against groups and websites that repeatedly share misinformation*, Harvard Kennedy School Misinformation Review (June 13, 2022), https://misinforeview.hks.harvard.edu/article/measuring-the-effect-of-facebooks-downranking-interventions-against-

groups-and-websites-that-repeatedly-share-misinformation/.

Notably, these successes depended on the use of algorithms to identify and remediate harmful content and to direct users to less-harmful content. Yet the use of algorithms to selectively present certain content to users is exactly the approach Petitioners urge should *not* be entitled to Section 230 immunity.

II. LIMITING SECTION 230 IMMUNITY WOULD DISCOURAGE ONLINE PLATFORM PROVIDERS FROM REMOVING OR DOWN-RANKING DANGEROUS CONTENT.

Petitioners' primary argument is that Section 230 should not shield online platforms from immunity when they use "complex automated recommendation systems" to display lists of content to a user. Pet'rs' Br. 17. They contend that injuries resulting from dangerous content that was discovered by virtue of being on such a list are attributable to the online platforms' conduct and that claims for redress from online platforms do not seek to treat the Defendant as the publisher or speaker of content created by a third party. *See* Pet'rs' Br. 27–33. Taking a similar tack, *amici* Former National Security Officials contend that "claims challenging [online platforms'] algorithmic amplification [of third-party content] do not attempt to 'treat[]' the platform as the 'publisher or speaker of [] information provided by another information content provider'" and thus do not implicate Section 230 immunity. Br. Former Nat'l Sec. Offs. 23. The Court's endorsement of this approach could have unintended consequences that harm our national security.

By their nature, online platforms perform numerous functions designed to promote some content and remove other content. Plainly, Congress understood this reality and took it into account when crafting the scope of Section 230 immunity: Section 230(f)(4), which defines "interactive computer service," makes clear that online platforms "(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."[2] And, regardless of whether providers do it via algorithm or manually, removing dangerous content from a platform does not occur in a vacuum; the act of deleting or downranking any one piece of content inherently has the effect of "promoting" everything else that *wasn't* removed or downranked. Likewise, redirecting users to alternative content arguably "promotes" or "recommends" that content. Thus, there is no such thing as neutrally eliminating *just* the bad online content; any step taken to address a particular video or post inevitably increases the relative predominance

---

[2] Indeed, operators of online platforms and publishers of traditional media are both largely in the business of directing users to particular content. For example, newspapers direct users to particular content by putting it above the fold on the first page or in the sports section. Because directing users to particular content is what publishers do, we respectfully disagree with the Solicitor General's assertion that, in attempting to hold YouTube liable for the manner in which it directed individuals to the relevant videos, Petitioners "do not seek to hold YouTube liable as a 'publisher' or speaker'" of the videos' contents. Br. U.S. 30.

of the posts that remain. And even if it were possible, proving that any such "promotion" was the result of removing or downranking dangerous content—and not from some other aspect of the ranking process—would be costly and complicated.

Moreover, online platforms like YouTube, Facebook, and Twitter organize and display vast amounts of user-generated content—far more than any workforce could manually and comprehensively review. Accordingly, operators of online platforms must use *some* form of automation to assist in reviewing third-party content and determining the circumstances under which to display a particular piece of third-party content on a list of material that is potentially relevant to the end user. In this connection, the Solicitor General correctly concluded that "YouTube's use of algorithms does not make it an 'information content provider' of the videos it recommends." Br. U.S. 30. As the SG explained, "the salient point is that the algorithms simply direct to particular users videos that were created and developed without YouTube's involvement." *Id.*

Moreover, it remains unclear whether alternatives to the user-interest-focused algorithms that many online platforms use today would be any better for national security—and they could be far worse. Take, for example, a system where user interaction alone (such as user "upvotes" or "downvotes" of third-party content) determines how content is displayed. Such an online platform would be using simple, non-algorithmic methods to "recommend" content and determine how prominently it is displayed. Under Petitioners' argument, then, the platform operator

would seemingly be entitled to Section 230 immunity for its recommendation lists. But terrorists and foreign adversaries have shown the will and the means to systematically "upvote" dangerous content. Rid, *supra*, at 400–410. They could easily exploit online platforms that organize third-party content by popularity. The same would be true if ranking were based on how often content is uploaded—terrorists and foreign adversaries could also manipulate that approach. *See id.*

For these reasons, we respectfully disagree with the claim that allowing Petitioners' claims to go forward "would not affect responsible content moderation efforts by social media platforms." Br. Former Nat'l Sec. Offs. 27. To the contrary, promoting content and removing or downranking content are two sides of the same coin. And it is necessary to rely in part on algorithms for such purposes because the amount of online material is much too large to be moderated by human reviewers alone.

Therefore, in our considered opinion, the best option is to encourage online platform providers to continue to improve their methods of detecting and responding to dangerous online material. Exposing them to liability under the circumstances of this case, where the nexus between the terrorists' actions and the actions of online platform providers is tenuous at best, would discourage providers from seeking to develop the most effective methods for identifying material that ought to be removed or downranked. Instead, the safe course for online platform providers would be to take a hands-off approach, which would

be contrary to the national security interests of the United States.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted,

Christopher J. Wright
Counsel of Record
Adrienne E. Fowler
John R. Grimm
HWG LLP
1919 M St NW #800
Washington, DC 20036
(202) 730-1325
cwright@hwglaw.com

JANUARY 19, 2023

Counsel for Amici Curiae

APPENDIX
LISTING OF *AMICI* IN ALPHABETICAL ORDER

Lieutenant General Joseph Anderson (USA-Ret.), Former Deputy Chief of Staff of the Army

Robert Cardillo, Former Director of the National Geospatial-Intelligence Agency

Lieutenant General James R. Clapper Jr. (USAF-Ret.), Former Director of National Intelligence

Lieutenant General Michael S. Groen (USMC-Ret.), Former Director of the Joint Artificial Intelligence Center

Commander Michael Lumpkin (USN-Ret.), Former Special Envoy/Coordinator at the U.S. State Department's Global Engagement Center

General Stanley McChrystal (USA-Ret.), Former Commander of U.S. and International Security Assistance Forces Afghanistan and Former Commander of the Joint Special Operations

Diane Rinaldo, Former Technology Policy Advisor for the House Permanent Select Committee on Intelligence and Former Acting Administrator of the National Telecommunications and Information Administration

David Shedd, Former Acting and Deputy Director of the Defense Intelligence Agency

Frances Townsend, Former Assistant to President George W. Bush for Homeland Security and Counterterrorism

Vice Admiral Timothy "TJ" White (USN-Ret.), Former Commander, U.S. Fleet Cyber Command, U.S. TENTH Fleet, U.S. Navy Space Command