No. 19-1284

IN THE

Supreme Court of the United States

MALWAREBYTES, INC.,
Petitioner,

v.

ENIGMA SOFTWARE GROUP USA, LLC,
Respondent.

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

BRIEF OF INTERNET ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

LAUREN GALLO WHITE
JONATHAN S.M. FRANCIS
Wilson Sonsini Goodrich & Rosati PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
lwhite@wsgr.com
jfrancis@wsgr.com

BRIAN M. WILLEN
Counsel of Record
Wilson Sonsini Goodrich & Rosati PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019
bwillen@wsgr.com

Attorneys for Amicus Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES (continued)

Page(s)

Constitutional Provisions

Statutes

Other Authorities

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

BRIEF OF INTERNET ASSOCIATION AS AMICUS CURIAE IN SUPPORT OF PETITIONER

Internet Association respectfully submits this brief as *amicus curiae* in support of Malwarebytes, Inc.'s petition for a writ of certiorari.[1]

INTEREST OF AMICUS CURIAE

The Internet Association ("IA") represents over 40 of the world's leading internet companies.[2] IA's mission is to foster innovation, promote economic growth, and empower people through a free and open internet.

IA has a powerful interest in the proper application of Section 230 of the Communications Decency Act ("Section 230"). IA members host enormous amounts of material uploaded by users, and they rely on Section 230 to protect their everyday operations, including their content-moderation efforts. IA submits this brief because it is concerned that the panel's decision, by misreading Section 230(c)(2)(B), threatens those efforts and will harm the quality of online platforms and the experiences of those who use them.

---

[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 or entity other than *amicus curiae* or its counsel has made a monetary contribution to the preparation or submission of this brief. All parties have consented in writing to the filing of this brief.

[2] IA's full membership is available at https://internetassociation.org/our-members.

INTRODUCTION AND SUMMARY OF ARGUMENT

Section 230 stands at the center of an ongoing debate over how online service providers should respond to objectionable, offensive, or dangerous content. The statute reflects Congress' judgment that the best way to protect online speech—and indeed the internet itself—is to allow platforms to set and enforce standards for appropriate speech on their services, and to do so generally free from either government censorship or the threat of private litigation.

In keeping with that purpose, Section 230 provides a pair of immunities that enable online service providers to host an enormous range of information and expression while simultaneously giving them the means to protect their users and themselves from objectionable material of all forms. These dual immunities have been vital to the development of online platforms and remain essential to their everyday operations. For the Internet Association (IA) and many of its member companies, Section 230 is foundational, a vital statute that protects both robust online speech and private editorial judgments. For all its importance, however, Section 230 has never been addressed by this Court. This case presents an ideal opportunity to do so.

This case involves Section 230(c)(2), a provision designed to ensure that online platforms have ample leeway to help screen users from a whole spectrum of unwelcome material, including threats of violence, hateful personal harassment, unwanted spam, poten-

tially harmful phishing or malware, and disinformation campaigns. As Congress explained, Section 230 was specifically enacted "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(3), (4).

The Ninth Circuit's decision in this case threatens this vital protection. Directly at issue is subsection 230(c)(2)(B), which immunizes online service providers' actions to "enable or make available . . . the technical means to restrict access to" a wide range of objectionable material. 47 U.S.C. § 230(c)(2)(B). This immunity focuses on tools that empower users to shield themselves from potentially harmful content. It ensures that providers do not face liability for creating and distributing technologies that let users block or filter content they may not want to see. IA's members and many other online service providers regularly rely on this immunity in developing and deploying a range of user-empowering tools, including Twitter's "block" and "mute" features, YouTube's Restricted Mode, Reddit's user-moderated forums, and Microsoft's Office 365 Advanced Threat Protection.

Defying basic rules of statutory interpretation, the Ninth Circuit engrafted onto this provision a requirement—conspicuously omitted from the statute's text—that courts consider the subjective motivations of online service providers before determining

whether the provider is entitled to the immunity Section 230(c)(2)(B) promises. In so doing, the Ninth Circuit exposes service providers to exactly the sort of costly litigation battles that the statute was intended to forestall. The petition for certiorari ably explains the legal failings of the Ninth Circuit's decision, and its conflict with the approach taken by other circuits. IA's brief explains the practical importance of Section 230(c)(2)'s protections, particularly for tools that help users make their own choices about objectionable online content. By misreading the statute, the Ninth Circuit has significantly weakened that protection, thereby putting a range of user-protection tools in peril and posing broader risks to service provider efforts to respond to harmful material. The Court should grant certiorari.

ARGUMENT

I. Section 230(c)(2) Was Designed to Protect Online Service Providers for Their Efforts to Regulate Online Content

Congress enacted Section 230 in significant part "to encourage interactive computer services and users of such services to self-police the Internet for obscenity and other offensive material, so as to aid parents in limiting their children's access to such material." *Batzel v. Smith*, 333 F.3d 1018, 1028 (9th Cir. 2003); *accord Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997) ("Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services."). The statute establishes as the "policy" of the United States "to encourage the development of tech-

nologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(3), (4). Congress intended the statute to spur the development of tools for screening objectionable content, and it sought to encourage those efforts by protecting online service providers from liability for claims based on those efforts.

To do so, Congress provided two robust immunities in Section 230(c)(2) : one for online service providers' decisions to directly restrict access to objectionable material; and one for their actions in making available to others the "technical means to restrict access" to such content. 47 U.S.C. § 230(c)(2)(A), (B). This approach facilitates private content regulation that helps protect internet users from potentially objectionable or harmful material, as well as from material that individuals may prefer to avoid for any number of reasons, such as concerns about age appropriateness, suitability for an office environment, or religious beliefs. Section 230(c)(2) accomplishes these goals while avoiding direct government regulation of online speech that may offend the First Amendment. *Accord Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 885 (1997). In this way, the statute forged a middle way between state-mandated censorship and an internet with no meaningful content moderation,

where children or other vulnerable groups may be exposed to objectionable (but constitutionally protected) material of all kinds. *See Batzel*, 333 F.3d at 1028.

"Rather than imposing penalties on Internet posters and their service providers," the proponents of Section 230 "argued that it would be more effective and fair to allow individuals and companies to set their own standards," and believed the market "would encourage the companies to develop conduct codes that are most appropriate for their audiences." Jeff Kosseff, The Twenty-Six Words That Created the Internet 63-64 (2019). As Representative Cox recognized when advocating for Section 230's passage, "this [content filtering] technology is very quickly becoming available, and in fact every one of us will be able to tailor what we see to our own tastes." 141 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox). His statements make clear that in passing Section 230, Congress sought "to help [the evolution of technology] ... by saying [that the] Government is going to get out of the way and let parents and individuals control it rather than [the] Government doing that job for us." *Id.*

In the more than two decades since Section 230 was enacted, courts have repeatedly recognized that Section 230 is to be read broadly, in accordance with the text of the statute and "[i]n light of Congress's objectives." *Force v. Facebook, Inc.*, 934 F.3d 53, 64 (2d Cir. 2019) (noting "general agreement that the text of [the CDA] should be construed broadly in favor of immunity"), *cert. denied*, No. 19-859, 2020 WL 2515485 (U.S. May 18, 2020); *Davison v. Randall*, 912 F.3d 666, 684 n.5 (4th Cir. 2019), *as amended* (Jan. 9, 2019)

("The federal Communications Decency Act allows private online intermediaries, like Facebook, the ability to moderate content by providing such intermediaries with broad immunity from user-generated content posted on their sites."); *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008) ("Courts have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content."); *Universal Commc'n. Sys. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007) ("In light of these policy concerns, we too find that Section 230 immunity should be broadly construed."); *Almeida v. Amazon.com*, 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted the CDA to establish broad federal immunity." (citation omitted)).

By failing to afford Section 230 an appropriately broad scope, the "specter of tort liability" would pose an "obvious chilling effect" on the "vibrant and competitive free market of ideas on the internet." *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009); *see also Fair Hous. Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008) (recognizing that close questions "must be resolved in favor of immunity").

II. Section 230(c)(2) Has Enabled Online Service Providers to Engage in Diverse and Valuable Content-Moderation Efforts

Operating under the protective framework established by Section 230(c), IA's members have developed a wide variety of content moderation tools and strategies. These come in two general forms. First, most if

not all online platforms affirmatively remove and block content—whether depictions of sexual exploitation, abusive bullying, or terrorist propaganda—that is at odds with the values of the particular platform, the law, or societal norms. Second, many online platforms offer tools that allow their users, or certain subsets of them, the freedom to screen or avoid content they may find objectionable and thereby tailor their own experiences.

A. Section 230(c)(2) Allows Platforms to Remove Unlawful and Offensive Content Without Fear of Liability

Most online service providers, including all of IA's members, have adopted policies prohibiting various forms of material or activities they deem harmful, inappropriate, or improper. The material covered by content policies is diverse: it includes various forms of pornography, abuse imagery, incitements to violence, fraudulent schemes, virulent hate speech, and material that advertises the sale of illegal goods and services.[3] In addition, IA members have rules against

---

[3] *E.g.*, *The Twitter Rules*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-rules; *Policies and Safety*, YOUTUBE, https://www.youtube.com/about/policies/#community-guidelines; *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards/; *Reddit Content Policy*, REDDIT, https://www.redditinc.com/policies/content-policy; *Community Guidelines*, https://www.linkedin.com/help/linkedin/answer/34593/linkedin-professional-community-policies?lang=en; *LinkedIn Professional Community Policies*, LINKEDIN, https://www.linkedin.com/help/linkedin/answer/34593/linkedin-

various forms of manipulation that can harm users, such as spam, malware, denial of service attacks, and hacking of user accounts. These rules are essential to protecting the provider's ability to reliably offer safe, secure, and functional services. Without them, online platforms would often become inhospitable places, where harmful and offensive material might drown out higher-quality speech. At the same time, different platforms can and do set different content rules, which reflect both wider social norms and the particular standards they wish to set for their specific online communities.

These rules will often change with the times, evolving as new challenges and social issues come to the fore. As the internet has matured, online service providers have developed policies and online tools to respond to an expanding range of threats. Very often, service providers have done so through tools that operate in the background, such as spam filtering, anti-virus, and anti-malware tools, as well as tools that

---

professional-community-policies?lang=en; *Community Guidelines*, PINTEREST, https://policy.pinterest.com/en/community-guidelines.

identify phishing scams[4] that trick users into providing valuable personal information.[5]

More recently, some providers have taken more public actions. For example, in light of the proliferation of misinformation about the recent novel coronavirus, COVID-19, Twitter announced it would remove Tweets that deny expert guidance, encourage the use of fake or ineffective treatments or preventions, or include misleading content purporting to be from experts or authorities.[6] Applying these policies, and enabled by Section 230's legal protections, Twitter has removed more than 2,600 Tweets containing misleading and potentially harmful content and has chal-

---

[4] *E.g.*, "The quiet evolution of phishing," MICROSOFT (Dec. 11, 2019), https://www.microsoft.com/security/blog/2019/12/11/the-quiet-evolution-of-phishing/ (discussing how Microsoft's Office 365 Advance Threat Protection team uses advanced security technologies to identify and prevent increasingly sophisticated phishing attacks).

[5] Section 230 inarguably protects these efforts to filter spam or prevent other manipulative behavior. *See Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (use of spam filtering technology and procedures to block mass marketing emails protected under Section 230(c)(2); *Holomaxx Techs. Corp. v. Yahoo!, Inc.*, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (same); *see also Roommates.com*, 521 F.3d at 1174 n.36 (9th Cir. 2008) (noting any filtering for spam would be protected by Section 230).

[6] V. Gadde & M. Derella, *An update on our continuity strategy during COVID-19*, TWITTER (Mar. 16, 2020), https://blog.twitter.com/en_us/topics/company/2020/An-update-on-our-continuity-strategy-during-COVID-19.html.

lenged more than 4.3 million accounts targeting discussions around COVID-19 with spammy or manipulative behaviors.[7]

The enforcement strategies of IA's members take many different forms, including manual review and automated systems, and they often require a staggering investment of resources. Some services allow users to flag potentially objectionable material, which is then manually reviewed by the service provider.[8] Some have dedicated teams that proactively monitor the platform looking for material that does not belong.[9] Some deploy sophisticated algorithms to help identify and block bad content.[10] The scope of these operations can be massive: larger services like YouTube, Twitter, and Facebook employ thousands of

---

[7] *Coronavirus: Staying safe and informed on Twitter*, TWITTER (Apr. 3, 2020), https://blog.twitter.com/en_us/topics/company/2020/covid-19.html#efforts

[8] *E.g.*, *Reporting Inappropriate Conduct*, YOUTUBE, https://support.google.com/youtube/answer/2802027?hl=en&ref_topic=9387085 (describing the various procedures and options users have "to flag content they find inappropriate" for review).

[9] *E.g.*, *Understanding the Community Standards Enforcement Report*, FACEBOOK, https://transparency.facebook.com/community-standards-enforcement/guide#section3 (explaining that "people on our trained teams proactively identify potential violations, focusing on harmful types of content").

[10] *E.g.*, *15th Transparency Report: Increase in proactive enforcement on accounts*, TWITTER (Oct. 2019), https://blog.twitter.com/en_us/topics/company/2019/twitter-transparency-report-2019.html (noting that "more than 50% of Tweets [Twitter] take[s] action on for abuse are now proactively surfaced using technology").

people around the world to review potentially objectionable content and apply their content-moderation policies to that content. And the use of these different review and enforcement strategies is constantly evolving. For example, with the onset of the COVID-19 pandemic and the enactment of social distancing measures, many online platforms announced they would rely more heavily on automated technology for content moderation.[11]

These policies and enforcement efforts result in the removal of large amounts of content, though this represents a small fraction of the overall amount of material posted on these platforms. For example, in the first six months of 2019, Twitter suspended a total of 244,188 unique accounts for violations related to child sexual exploitations; much of this work was facilitated by technology such as PhotoDNA, which helps identify child sexual exploitation and abuse imagery in an automated way.[12] Similarly, in 2019, Red-

---

[11] E.g., Gadde & Derella, supra note 6 (Twitter was increasing use of machine learning and automation to act on abusive and manipulative content); *Protecting our extended workforce and the community*, YOUTUBE (Mar. 16, 2020) https://youtube-creators.googleblog.com/2020/03/protecting-our-extended-workforce-and.html (YouTube would rely more on technology to detect and assess potentially harmful content).

[12] *New Technology Fights Child Porn by Tracking its "PhotoDNA"*, MICROSOFT (Dec. 15, 2009), https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/#sm.0001mpmupctevct7pjn11vtwrw6xj. This technology is widely used by IA members, including Google, Twitter, Facebook, Reddit, Microsoft, and numerous other or-

dit's in-house content administrators (Admins) removed 222,309 pieces of content for violations of Reddit's Content Policy, including harassment, minor sexualization, violent content, and others.[13] Over the same time period, Microsoft's email services blocked over 13 billion malicious and suspicious phishing emails, over 1 billion of which contained novel URL-related phishing threats. Meanwhile, in the final three months of 2019 alone, YouTube removed almost six million videos from its service for violating its community guidelines.[14] And in the first quarter of 2020, Facebook removed 9.6 million pieces of content that violated its prohibition on hate speech.[15]

---

ganizations. And in recent years, many of IA's members have expanded the use of the technology to identify and remove terrorist content online. See *Partnering to Help Curb Spread of Online Terrorist Content*, FACEBOOK (Dec, 5, 2016) https://about.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/.

[13] *Transparency Report 2019*, REDDIT, https://www.redditinc.com/policies/transparency-report-2019. This number excludes spam and other types of content manipulation removals that are done at scale through automated means, as well as content removed for violations of copyright and other legal removals. *Id*.

[14] *YouTube Community Guidelines enforcement*, GOOGLE, https://transparencyreport.google.com/youtube-policy/removals?hl=en.

[15] *Community Standards Enforcement Report*, FACEBOOK, https://transparency.facebook.com/community-standards-enforcement#hate-speech.

B. Section 230(c)(2)(B) Encourages Platforms to Develop Tools that Empower Users to Curate Their Own Online Experiences

Beyond protecting the efforts of online service providers to directly block or remove objectionable material, Section 230 also facilitates valuable content-moderation in another way. Subsection (c)(2)(B) protects service providers for making available tools that enable their users to curate their online experience or avoid content they may not want. This provision immunizes "any action taken to enable or make available to information content providers or others the technical means to restrict access" to content that they consider objectionable. 47 U.S.C. 230(c)(2)(B).

Like the direct content-moderation techniques discussed above, the user-empowerment tools covered by Section 230(c)(2)(B) take diverse forms. For example, YouTube's Restricted Mode is an optional, opt-in setting that allows sensitive users (including parents, libraries, and schools) to avoid videos that may be inappropriate for some audiences, including those depicting alcohol or drug use, frank discussions of sexuality, and descriptions of violence or political conflicts.[16] YouTube uses a combination of automated systems and manual reviewers to rate and label videos as "Teen" or "Mature," which will not be shown to users who have chosen to turn on Restricted Mode.

---

[16] See *Disable or enable Restricted/Safe Mode*, YOUTUBE, https://support.google.com/youtube/answer/174084; *Your content & Restricted Mode*, Google, https://support.google.com/youtube/answer/7354993?hl=en.

Restricted Mode is precisely the kind of tool that Congress wanted Section 230 to protect: it allows YouTube to keep its general service open to a wide range of material, including potentially mature videos that may offend some people, while allowing users who don't wish to see such content to have a more limited YouTube experience.

Twitter offers a different set of tools that aim at a similar purpose. Twitter users can choose to "Block" or "Mute" users whose Tweets they wish to avoid or who they may find objectionable.[17] Through blocking, a user can restrict another Twitter account from contacting them or seeing their Tweets. Muting allows users to shield themselves from certain users or from Tweets that contain particular content, such as words or phrases that a user finds offensive or simply does not wish to see.[18] Through these tools, which are another paradigm of what Section 230(c)(2)(B) covers, Twitter gives its users the ability to curate their personal experience on the service based on their individual preferences.

---

[17] See *How to mute accounts on Twitter*, TWITTER, https://help.twitter.com/en/using-twitter/twitter-mute; *How to block accounts on Twitter*, Twitter, https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts.

[18] For example, the U.K.'s Gambling Commission provides recommendations to gambling addicts on how to limit gambling content from a Twitter feed using these tools. *Controlling the level of gambling-related content you see on Twitter*, UK Gambling Commission, https://www.gamblingcommission.gov.uk/for-the-public/Safer-gambling/Consumer-guides/Controlling-the-level-of-gambling-related-content-you-see-on-Twitter.aspx.

Similarly, on Reddit—an online network of diverse, user-run communities—content regulation depends heavily on volunteer user moderators using tools supplied by Reddit.[19] Moderators in each community set rules that fit their specific circumstances, which they enforce via a suite of tools that enable manual removal of individual rule-breaking posts or comments; automatic removal of individual posts or comments according to moderator-configurable rules; and temporary or permanent banning of rule-breaking users from posting or commenting in the community.[20] Reddit also gives its users tools allowing them to opt-out of seeing material labeled "NSFW" (not safe for work) and to control (via an opt-in mechanism) whether they see material from "quarantined" communities, which contain material that average users may find highly offensive or upsetting.[21] The diversity of these Reddit sub-communities illustrates that content-moderation practices differ according to circumstances and are not always focused on objectively "offensive" content; at times, they aim at content that simply is not suitable for a given forum. For example, the subreddit "Cats Standing Up" (r/catsstandingup)

---

[19] More than 99% of the pieces of content removed from Reddit in 2018 were removed by volunteer user moderators using Reddit-provided tools. See *Transparency Report 2018*, REDDIT, https://www.redditinc.com/policies/transparency-report-2018.

[20] See *Moderation Tools – overview*, REDDIT, https://mods.reddithelp.com/hc/en-us/articles/360008425592-Moderation-Tools-overview.

[21] See *Quarantined Subreddits*, REDDIT, https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/quarantined-subreddits.

only allows users to post photos of cats standing up; posts may be removed if they depict a cat sitting down — or a standing animal that is not a cat. Section 230(c)(2)(B) protects all of this: it enables providers to supply users with tools to tailor their own experiences and create online communities of their own choosing.

Section 230(c)(2)(B) also applies outside the context of user-submitted content on public websites and social-media services. For example, and critically important to anyone with an email account, Section 230(c)(2)(B) facilitates the use of tools that filter tens of billions of unwanted spam messages from email and other online services. These anti-spam tools often forgo a one-size-fits-all approach in lieu of customizable settings, supplementing the service providers' own decisions to directly block spam or other unwanted content under the protections of Section 230(c)(2)(A). *See, supra* Part II.A. For example, Google's Gmail allows users to adjust their individual experiences, including by blocking senders based on email address or domain or creating email block lists and safe lists, amongst others.[22] Microsoft's Defender Antivirus and its Defender SmartScreen similarly allow users to tailor their malware protection to meet their individual needs, such as through altering the protection afforded for particular folders or excluding certain files from antivirus scanning.

These tools are integral for the vitality of online services and communities. They ensure that diverse

---

[22] *Spam Settings*, GOOGLE, https://support.google.com/a/topic/2683828?hl=en&ref_topic=2683865.

content can flourish and find its appropriate audience, and they allow users to curate their own online experiences and choose to avoid certain content. They allow providers to protect their systems and users from a range of threats: from financial scams and ransomware attacks to spam and phishing attempts. That these tools have developed under the framework established by Section 230 illustrates the wisdom and foresights of the legislative choice Congress made in the early days of the internet.

C. Section 230(c)(2) Must Be Broadly Construed to Protect the Self-Regulatory Tools Used by Online Platforms and Their Users

Critically, the efficacy of such tools and content moderation efforts depends on service providers and users having the freedom to determine for themselves what material they find objectionable. Content that may be objectionable for some platforms, communities, or users might not be objectionable for others.

Section 230(c)(2) recognizes and accommodates this reality in two ways. *First*, the material that is covered by the provision is not limited to the specific categories listed in the statute ("obscene, lewd, lascivious, filthy, excessively violent, [and] harassing") but extends to any material that is "otherwise objectionable," regardless of whether it is "constitutionally protected." 47 U.S.C. § 230(c)(2)(A). Even the Ninth Circuit's decision below recognized that this catchall is broad and cannot be limited to material "that is sexual or violent in nature." Pet. App. 21a. Instead, it

"was more likely intended to encapsulate forms of unwanted online content that Congress could not clearly identify in the 1990s." *Id.* at 49a.

Second, the statute imposes a subjective, rather than an objective, standard for evaluating whether material falls into these categories. What matters is not whether the material is "otherwise objectionable," but instead whether the "provider or user *considers*" it to be so. 47 U.S.C. § 230(c)(2)(A) (emphasis added). The decision below recognized that as well. Pet. App. 5a. ("[Section 230(c)(2)] establishes a subjective standard whereby internet users and software providers decide what online material is objectionable."). In these ways, Section 230(c)(2) eschews a one-size-fits-all approach. Instead, it imposes a flexible standard that allows service providers and users to establish their own "standards of decency without risking liability for doing so." *Green v. AOL*, 318 F.3d 465, 472 (3d Cir. 2003).

Under these protections, different online communities can set different content standards, confident of the immunity Section 230(c)(2) provides. An online forum dedicated to promoting veganism may find advertisements for beef or postings celebrating hunting to be "objectionable" even if those would be entirely appropriate on another platform. Likewise, religious users may consider objectionable discussions of sexuality or reproductive freedom that others may welcome. Section 230 takes these nuanced, context-specific decisions out of the hands of the government and the courts, instead empowering service providers and their users to act based on their own sensibilities and standards.

III. The Ninth Circuit's Decision Undermines the Goals of Section 230 and Threatens Valuable Content Moderation Tools

Against this background, the Ninth Circuit's decision in this case is dangerous. While there was much the panel got right about Section 230, its basic holding—that Section 230(c)(2)(B) does not protect "blocking and filtering decisions that are driven by anticompetitive animus"—threatens to undermine the important self-regulatory efforts that Section 230 is intended to facilitate. In reaching that conclusion, the panel, over Judge Rawlinson's trenchant dissent, effectively read into Section 230(c)(2)(B) an intent-based limitation. The majority's holding means that a service provider may lose immunity for providing an otherwise protected filtering tool based on the mere allegation that the service provider (or user) allegedly acted with an improper motive or purpose.

The Ninth Circuit's ruling defies core principles of statutory interpretation. Section 230(c)(2)(B) forgoes the kind of purpose-based, good faith requirement the Ninth Circuit read into that provision. That is clear from the contrast between subsection (c)(2)(A) and (c)(2)(B). While the former includes an express "good faith" requirement, the latter conspicuously excludes one. "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States*, 464 U.S. 16, 23 (1983) (citation omitted)). This established rule should have controlled the Ninth Circuit's decision. The obvious omission of good faith language

from subsection (c)(2)(B) confirms that the immunity does not turn on any consideration of good faith—whether in the form of an anticompetitive motive or otherwise. That is why the panel majority's decision was quickly rejected by a California state court in *Prager University v. Google LLC*, No. 19-cv-340667, 2019 Cal. Super. LEXIS 2034 (Super. Ct. Cal. Nov. 19, 2019). As the state court explained, echoing Judge Rawlinson's dissent, the panel "ignore[s] the plain language of the statute by reading a good faith limitation into Section 230(c)(2)(B)." *Id*. at *26.

Congress had good reason to omit a good faith requirement from subsection (c)(2)(B). As discussed above, subsection (A) protects direct blocking or filtering by online service providers—situations where providers act unilaterally to protect themselves or their users from objectionable material. *See Batzel*, 333 F.3d at 1030 n.14. In contrast, subsection (B) only applies where service providers put blocking tools in the hands of users, who must independently and affirmatively decide to use those tools. Here, blocking does not occur unilaterally; it instead requires cooperation between a service provider and a third party. *Id.* at 1029 ("Some blocking and filtering programs depend on the cooperation of website operators and access providers who label material that appears on their services.").

In this scenario, Congress logically concluded it was unnecessary to include a good faith requirement or to allow Section 230's protection to turn on disputes about a service provider's motives. Here, the user's independent choice operates as a check on the provider's decisions about what material should be filtered or

blocked. This vital element of user choice under 230(c)(2)(B) was recognized in *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009): "If a Kaspersky user (who has bought and installed Kaspersky's software to block malware) is unhappy with the Kaspersky software's performance, he can uninstall Kaspersky and buy blocking software from another company that is less restrictive or more compatible with the user's needs." *Id.* at 1177.

The panel's refusal to similarly apply the plain language of the statute in this case threatens to significantly water-down the Act's "robust" immunity. *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003). The decision here gives plaintiffs seeking to evade Section 230(c)(2)'s protections an easy way to try to do so: under *Enigma*, plaintiffs need only make vague allegations of anti-competitive motive to state a claim and require online service providers to engage in time-consuming, expensive, and asymmetrical discovery. This threat is not hypothetical: parties upset that their material has been blocked or filtered will often assert—without any legitimate support or factual basis—that the decision was driven by animus. We have already seen this, with a party suing YouTube for excluding some of its videos via YouTube's Restricted Mode and alleging—to escape Section 230(c)(2)(B)—that because YouTube creates some original content, it must somehow be "competing" with the plaintiff and acting with anti-competitive motive. *See Prager*, 2019 Cal. Super. LEXIS 2034, at n 4.

Allowing this gambit undermines a core aim of Section 230: to protect "websites not merely from ultimate liability, but from having to fight costly and protracted legal battles." *Roommates.com*, 521 F.3d at 1175. And it contradicts the uniform rule that courts must "aim to resolve the question of § 230 immunity at the earliest possible stage of the case." *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 255 (4th Cir. 2009) (citing *Roommates.com*, 521 F.3d at 1175). Courts should not "cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites." *Roommates.com*, 521 F.3d at 1174. Unfortunately, the Ninth Circuit lost sight of that important precept here. This Court should take this opportunity to confirm that Section 230 cannot be so readily avoided. Under Section 230(c)(2)(B), inquiries into the "real" purpose of the blocking are unnecessary—and inappropriate. Indeed, if plaintiffs can sidestep Section 230 at the pleading stage in this way, the immunity loses much of its value. *Accord Nemet*, 591 F.3d at 255 (recognizing that Section 230 immunity from suit "is effectively lost if a case is erroneously permitted to go to trial") (citation omitted).

Based on barebones allegations, service providers (and even users) may be threatened with expensive and time-consuming litigation to defend their self-regulatory efforts—efforts that happen constantly, given the massive scale of online communications. As much as the actual risk of liability, such litigation burdens significantly raise the costs of engaging in self-regulation, and some providers may find that the risk is simply not worth it. Faced with potential discovery into the subjective motivations associated with

every tool they offer to users to help filter or curate content—platforms will inevitably pull back from providing such tools to avoid burdensome litigation. That, of course, is the opposite of how Section 230 is supposed to work. One of the "principal benefit[s]" of Section 230 is the promise "of fast, cheap, and reliable defense wins." Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. Irvine L. Rev. 659, 671 (2012). Given the sheer scale of online communication, the risk of litigation for content moderation efforts may both discourage larger platforms from allowing diverse expression, while also preventing newer and smaller service providers from obtaining the investment necessary to enter the market.

In short, the Ninth Circuit's approach will discourage rather than "encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools," 47 U.S.C. § 230(b)(3), and it will create rather than "remove disincentives for the development and utilization of blocking and filtering technologies," *id.* § 230(b)(4). Certiorari should be granted to give effect to Congress' goal of ensuring that online platforms continue to develop and make available to users filtering tools to allow users a freedom of choice in curating their own individual experience on the internet.

CONCLUSION

For the foregoing reasons, the Court should grant Malwarebytes's petition for a writ of certiorari.

Respectfully submitted,

LAUREN GALLO WHITE
JONATHAN S.M. FRANCIS
Wilson Sonsini Goodrich
& Rosati PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
lwhite@wsgr.com
jfrancis@wsgr.com

BRIAN M. WILLEN
Counsel of Record
Wilson Sonsini Goodrich
& Rosati PC
1301 Avenue of the
Americas, 40th Floor
New York, NY 10019
bwillen@wsgr.com

Counsel for Amicus Curiae

June 12, 2020