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 IN OPPOSITION FOR RESPONDENT

CHRISTOPHER M. VERDINI
ANNA SHABALOV
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
(412) 355-6500

TERRY BUDD
Counsel of Record
BUDD LAW, PLLC
120 Lyndhurst Circle
Wexford, PA 15090
(412) 613-2541
(terry.budd@buddlawglobal.com)

July 27, 2020

QUESTION PRESENTED

Whether the Ninth Circuit correctly held that 47 U.S.C. § 230(c)(2), titled "Protection for 'Good Samaritan' blocking and screening of offensive material," does not provide immunity from liability for companies engaging in predatory practices that intentionally target competitors for anticompetitive reasons.

RULE 29.6 DISCLOSURE STATEMENT

Enigma Software Group USA, LLC is a Florida limited liability company with its principal place of business in Florida. Enigma Software Group USA, LLC is 100% owned by Globalist LLC, a Delaware limited liability company. Globalist LLC has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

CONSTITUTION, STATUTES, AND RULES

LEGISLATIVE MATERIALS

ADMINISTRATIVE MATERIALS

OTHER MATERIALS

INTRODUCTION

Petitioner Malwarebytes, Inc. ("Malwarebytes") maliciously targeted its direct competitor, respondent Enigma Software Group USA, LLC ("Enigma"), by programming its software to designate Enigma's legitimate and highly regarded cybersecurity programs as "threats." Malwarebytes blocked the installation, operation, and use of Enigma's software for users who sought to download, and in some instances already had paid for, Enigma's programs. Malwarebytes then claimed immunity for these predatory, unfair tactics under Section 230 of the Communications Decency Act of 1996 ("CDA"), a provision intended to protect "Good Samaritan" blocking of "objectionable" online material. The Ninth Circuit rejected Malwarebytes' immunity defense, ruling that Section 230 immunity does not extend so broadly as to immunize blocking of direct competitors for anticompetitive reasons.

That common-sense, textually grounded holding is sound. In its certiorari petition, Malwarebytes identifies no direct Circuit split. Instead, it seeks to conjure a conflict on general Section 230 approaches and an alleged split with a California state trial court case. Those arguments fail because this case is one of first impression as to whether Section 230 extends immunity from liability for companies engaged in anticompetitive targeting of direct competitors.

Moreover, the Ninth Circuit's holding applies in a narrow and fact-bound circumstance. Contrary to Malwarebytes' fictional doomsday scenarios, it will not have far-reaching impact on Section 230 jurisprudence or on the protections on which companies operating on the Internet rely. Malwarebytes can identify no other cases involving companies claiming immunity for similar tactics. The petition should be denied.

STATEMENT

I. STATUTORY CONTEXT

In 1996, when the Internet was a nascent technology, Congress responded to concerns about the exposure of children to the obscenity and pornography flooding the web by passing the CDA. Section 230 of the CDA empowers providers of interactive computer services to block obscene and pornographic content themselves and incentivizes them to provide tools that would enable parents to protect their children, by immunizing the providers against certain types of claims. *See Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003) ("The primary goal of the Act was to control the exposure of minors to indecent material."), *superseded by statute on other grounds as recognized by Breazeale v. Victim Servs., Inc.*, 878 F.3d 759 (9th Cir. 2017).

Congress expressed policies central to Section 230's governance of the Internet:

> It is the policy of the United States—
>
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
>
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

47 U.S.C. § 230(b).

To further those express policies, Congress created an immunity under Section 230(c)(2), entitled "Protection for '***Good Samaritan***' blocking and screening of offensive material" (emphasis added), which specifies:

> 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 ([A]).[1]

---

[1] Although the statutory text references "material described in paragraph (1)," this is "a typographical error, and . . . instead the reference should be to paragraph (A), i.e., § 230(c)(2)(A)." *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 n.5 (9th Cir. 2009).

Id. § 230(c)(2). *See also Batzel*, 333 F.3d at 1028 (Section 230(c) was enacted "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").

II. FACTUAL BACKGROUND

As alleged in Enigma's operative Complaint, Enigma is an established cybersecurity company whose cybersecurity products have protected millions of users from computer viruses, malware, hackers, system breaches, and identity theft. *See* First Am. Compl. ¶¶ 2, 46, *Enigma Software Grp. USA, LLC v. Malwarebytes Inc.*, No. 1:16-cv-7885, Dkt. 33 (S.D.N.Y. Dec. 7, 2016) ("Compl."). Enigma's offerings have included a flagship anti-malware product, SpyHunter 4, and an advanced Windows optimizer and repair program, RegHunter 2. *Id.* ¶¶ 46-47. Both programs have received top industry certifications. *Id.* ¶ 52.

Enigma and Malwarebytes are direct competitors in the anti-malware and cybersecurity market. *Id.* ¶¶ 3-4, 54. Malwarebytes' flagship anti-malware product, MBAM, competed directly with SpyHunter 4.[2] *Id.* ¶¶ 4, 54. Malwarebytes markets and promotes its MBAM product through, *inter alia*, an affiliate program, in which it pays its affiliates commissions for purchases of MBAM that users make through the affiliates' websites. *Id.* ¶¶ 22, 61.

---

[2] SpyHunter 4 was phased out of the market after Enigma's affiliate, EnigmaSoft Limited, introduced the new SpyHunter 5 anti-malware product in June 2018. Malwarebytes' MBAM now competes directly with SpyHunter 5.

On January 5, 2016, Enigma filed suit against Bleeping Computer LLC ("Bleeping"), one such Malwarebytes affiliate, to seek redress for Bleeping's deliberate dissemination of false and misleading information about Enigma and SpyHunter 4 (the "Related Case"). *Id.* ¶¶ 21, 23, 61. Bleeping operated a website at www.bleepingcomputer.com that it held out to computer users as an independent, objective source of cybersecurity information, including anti-malware software product reviews. *Id.* ¶ 61. In reality, however, Bleeping acted as a sales arm for Malwarebytes, receiving commissions from sales of MBAM it originated on its website. *Id.* ¶¶ 22, 61. To increase its earnings and to build business benefiting itself and Malwarebytes, Bleeping undertook a concerted smear campaign against Enigma, in which it made multiple posts on its site that: (i) made repeated defamatory statements about Enigma and its products, (ii) instructed consumers not to install SpyHunter and provided instructions on how to uninstall SpyHunter for those who already had the product, and (iii) directed users to instead purchase MBAM. *Id.* ¶¶ 23, 61. Bleeping earned commissions on the sales of MBAM it generated in this fashion, and Malwarebytes in turn directly profited from the concerted unlawful conduct through increased sales and greater exposure on a well-regarded and ostensibly independent website. *Id.* ¶¶ 22, 62. In recognition of their partnership, Malwarebytes even funded a portion of Bleeping's defense costs in the Related Case. *Id.* ¶ 64.

As part of discovery in the Related Case, Enigma served Malwarebytes with a Rule 45 subpoena seeking documents that would establish Malwarebytes' deep relationship with Bleeping and its collaboration with Bleeping's efforts to divert sales from Enigma to

Malwarebytes (the "Subpoena"). *Id.* ¶¶ 21, 24, 66. On October 5, 2016, ***less than a week before its response to the Subpoena was due***, Malwarebytes—facing the prospect of having to produce documents to Enigma and testify under oath regarding its involvement in Bleeping's anticompetitive conduct and at risk of losing the competitive advantages provided by Bleeping's smear campaign—publicly announced that it had amended the "criteria" it used to define "potentially unwanted programs" ("PUPs") to include a series of factors that largely tracked Bleeping's defenses and counterclaim allegations about Enigma in the Related Case. *Id.* ¶¶ 7, 21, 25-27, 67, 71-73.

Simultaneously, for the first time, Malwarebytes began to characterize Enigma's programs as PUPs and "threats." *Id.* ¶¶ 25, 72-73. Notably, from Malwarebytes' inception in 2008 through October 6, 2016—during eight years of direct competition—Malwarebytes had never identified Enigma's programs as PUPs or any other type of "threat." *Id.* ¶¶ 6-7. Malwarebytes' use of its "revised" PUP criteria as a pretext to target Enigma was transparent; when, within hours of Malwarebytes' announcement, Bleeping posted on its website a front-page news article about the "revised" PUP criteria, a user commented: "What would be really strange is if anyone can think of any other anti-malware program that fits any one of those descriptions [the PUP criteria] …. not that I can think of one of course :)." *Id.* ¶ 31 (alterations in original).

Having characterized Enigma's SpyHunter 4 and RegHunter 2 as "PUPs" and "threats," Malwarebytes' MBAM began, also for the first time in its existence, to block users' installation and use of Enigma's

products. *Id.* ¶¶ 6, 9, 16, 81.[3] Users (many of whom had already paid for Enigma's programs) attempted unsuccessfully to opt-out of Malwarebytes' disabling "quarantine" of Enigma's products and were trapped by MBAM in unproductive cycles of repeated blocking. *Id.* ¶¶ 10-11, 17, 86-89, 93-95.

When it decided to block Enigma's programs, Malwarebytes knew that Enigma's programs were legitimate, posed no security threat to users' computers, and were not harassing in any way. *Id.* ¶¶ 124-125. Malwarebytes had, and has, no objective, good-faith basis to claim that Enigma's programs—that consumers have chosen to download and purchase—are "potentially unwanted" or a "threat." *Id.* ¶¶ 18, 126-127. No such basis exists. *Id.* Malwarebytes' "revision" of its PUP criteria was a mere pretext under which it blocked user access to Enigma programs, gained an unfair business advantage, furthered its anticompetitive scheme, and retaliated against Enigma for the Subpoena in the Related Case, which

---

[3] For consumers who had already installed and paid for Enigma's programs, MBAM "quarantined" Enigma program files as PUPs in a "Total Threats Detected" window, preselected the files for removal, and prompted the user to remove them via a "Remove Selected" button. Compl. ¶¶ 82-84. Regardless of whether the user clicked "Remove Selected," MBAM prevented the launch of Enigma programs. *Id.* ¶ 85. For consumers who attempted to newly download Enigma products, MBAM blocked the installer files and prevented their installation. *Id.* ¶ 92. The only way a user could stop the unproductive cycle of trying and failing to exclude Enigma's programs from "quarantine" was by adding the Enigma files to a "Malware Exclusion" list within MBAM's settings, a step that is wholly counterintuitive because neither Enigma's products nor PUPs generally (however defined) are malware. *Id.* ¶¶ 90-91. And, even if a user knew how to do this, MBAM would continue to characterize and quarantine other Enigma files as PUPs and "threats." *Id.*

would have exposed Malwarebytes' involvement in Bleeping's smear campaign against Enigma. *Id.* ¶¶ 7-8, 21, 24-27, 67, 72-73, 76, 127.

Indeed, Malwarebytes' own employees made clear the targeted nature of Malwarebytes' "revised" PUP criteria. One Malwarebytes employee (and developer of AdwCleaner, an anti-adware product acquired by Malwarebytes shortly after it announced its revised PUP criteria) specifically called out Enigma, and only Enigma, in a tweet about Malwarebytes' "revised" PUP approach: "#AdwCleaner by @Malwarebytes now fully detects and removes #SpyHunter from Enigma Software Group #PUP." *Id.* ¶¶ 32, 78. The following day, a user of Malwarebytes' forum website posted a link to that tweet. *Id.* ¶ 33. A Malwarebytes "Expert" responded: "Nice way to exacerbate things when Enigma has already filed suit against Malwarebytes. It's one thing quietly removing Enigma'ware. It is another announcing it, in public, after a suit has already been filed." *Id.* He continued, in a second post, to highlight the targeted nature of Malwarebytes' attack: "***WHY*** tweet it? If there are 15,1000 [sic] PUPs that are current, should we expect 15,000 tweets for each and every one? It isn't like some major BOTnet takedown or something of that nature. Why exacerbate the issue after a lawsuit was filed in US Federal Court?" *Id.* (alteration in original).

III. PROCEDURAL HISTORY

A. District Court Opinion

After Malwarebytes revised its PUP criteria and first began characterizing, quarantining, and blocking SpyHunter 4 and RegHunter 2 as PUPs and "threats," Enigma sued Malwarebytes in the United States District Court for the Southern District of New York,

bringing claims of Lanham Act false advertising, violations of New York General Business Law § 349, tortious interference with contractual relations, and tortious interference with business relations. *See* Compl., No. 1:16-cv-7885, Dkt. 1 (S.D.N.Y. Oct. 7, 2016). The court designated the case as related to the Related Case, already pending in that district. After Enigma and Bleeping settled and the Related Case was terminated, the court granted Malwarebytes' request for a transfer to the Northern District of California pursuant to 28 U.S.C. § 1404.[4] *See id.*, Dkt. 67.

Upon transfer, Malwarebytes renewed a Rule 12(b)(6) motion to dismiss ("Motion"), arguing that Enigma had failed to state a claim for two distinct reasons: (1) Malwarebytes was immune from all of Enigma's claims under Section 230(c)(2) of the CDA, and (2) Enigma had failed to sufficiently plead the elements of its substantive claims. *See* No. 5:17-cv-2915, Dkts. 97, 100, 102 (N.D. Cal.).

On November 7, 2017, the district court granted Malwarebytes' Motion and dismissed Enigma's Complaint with prejudice. Pet. App. 57a-65a. The court's sole ground for dismissal was Malwarebytes' purported immunity under Section 230(c)(2)(B). *Id.* at 65a. The court held that *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009), required dismissal of Enigma's claims. Pet. App. 62a. It read *Zango* as permitting a provider of interactive computer services such as Malwarebytes to unilaterally deem any content "objectionable" and block it without having to

---

[4] Malwarebytes also moved to dismiss under Rule 12(b)(2) for lack of personal jurisdiction and Rule 12(b)(6) for failure to state a claim. *See* Dkts. 37-42. The district court expressly declined to decide the Rule 12(b) motions. *See* Dkt. 67, at 19.

account for its actions or the harm it caused to consumers and competitors. *Id.* The court did not reach Malwarebytes' arguments as to the adequacy of Enigma's pleading on its substantive claims.

B. Ninth Circuit Opinion

The Ninth Circuit reversed the district court's dismissal of Enigma's claims. *See* Pet. App. 30a-54a. The court of appeals determined that *Zango* was not dispositive; although *Zango* determined that "providers have discretion to identify what online content is considered 'objectionable,'" it did not "discuss the scope of that discretion." *Id.* at 39a. The Ninth Circuit further found that Malwarebytes' claim of unfettered authority to block direct competitors was "contrary to CDA's history and purpose." *Id.* at 47a. The Ninth Circuit concluded:

> Because we hold that § 230 does not provide immunity for blocking a competitor's program for anticompetitive reasons, and because Enigma has specifically alleged that the blocking here was anticompetitive, Enigma's claims survive the motion to dismiss. We therefore reverse the dismissal of Enigma's state-law claims and we remand for further proceedings.

Id. at 50a-51a.

The Ninth Circuit denied Malwarebytes' en banc request, with no judge requesting a vote on whether to rehear the case en banc. *Id.* at 4a. The panel also issued an amended opinion, *id.* at 5a-27a ("Ninth Circuit Opinion"), modifying, at Malwarebytes' request, one sentence of its original opinion. *Compare id.* at 39a *with id.* at 11a; *see infra* note 10.

REASONS FOR DENYING THE PETITION

I. THE NINTH CIRCUIT'S DECISION WAS CORRECT

A. The Ninth Circuit's Judgment Is Consistent with the Statutory Text

Section 230(c)(2)(B) is part of a subsection of Section 230 titled "Protection for 'Good Samaritan' blocking and screening of offensive material." It provides that "[n]o provider or user of an interactive computer service shall be held liable on account of" "any action taken to enable or make available to information content providers or others the technical means to restrict access to" "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c)(2)(A), (B). "[O]therwise objectionable" is not further defined in the statute, but Congress "took the rather unusual step," Pet. App. 10a-11a, of including in the text of Section 230 a series of ***express*** "polic[ies] of the United States" underpinning the statute, 47 U.S.C. § 230(b). *See supra* pp. 2-3.

The Ninth Circuit held that "otherwise objectionable" did not extend to cover material from a direct "competitor" that an interactive computer service blocks for "anticompetitive reasons." Pet. App. 23a. The court presented a two-prong test for evaluating motions to dismiss claiming Section 230(c)(2)(B) immunity for blocking material as "otherwise objectionable": a plaintiff can survive the motion only if it adequately pleads both that (i) it is the defendant's direct competitor and (ii) the defendant specifically targeted the plaintiff's material for anticompetitive reasons.

The Ninth Circuit further explained, in detail, how Section 230's expressly stated policies supported this common-sense limitation on "otherwise objectionable":

> Congress expressly provided that the CDA aims "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services" and to "remove disincentives for the development and utilization of blocking and filtering technologies." § 230(b)(2)–(3). Congress said it gave providers discretion to identify objectionable content in large part to protect competition, not suppress it. *Id.* In other words, Congress wanted to encourage the development of filtration technologies, not to enable software developers to drive each other out of business.
>
> . . .
>
> We must today recognize that interpreting the statute to give providers unbridled discretion to block online content would . . . enable and potentially motivate internet-service providers to act for their own, and not the public, benefit. Immunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy. *See* § 230(b)(3) (to maximize user control over what content they view). Indeed, users selecting a security software provider must trust that the provider will block material consistent with that user's desires. Users would not reasonably anticipate providers blocking valuable online content in order to stifle competition. Immunizing anticompetitive blocking would, therefore,

> be contrary to another of the statute's express policies: "removing disincentives for the utilization of blocking and filtering technologies." *Id*. § 230(b)(4).

Id. at 19a-21a (citation omitted).

As the Ninth Circuit properly recognized, Congress did not write Section 230(c)(2) in such a boundless fashion as to immunize companies from liability for attacks against direct competitors that are motivated by anticompetitive animus and that violate a wide range of long-established laws and precedent against unfair competition, false advertising, and tortious interference. And Congress did not shield such unlawful anticompetitive acts under the auspices of a "Good Samaritan" statute when those acts disregard, and in fact are directly harmful to, the interests of the very users Section 230 was designed to protect.

Indeed, the Ninth Circuit Opinion comports with a long-established cornerstone of the U.S. free market economy: that, to foster innovation and provide consumers with increased choice, companies ought to be free to compete based on the merits of their products, without facing destruction at the hands of larger, better-resourced companies through anticompetitive targeting. *See Nat'l Soc'y of Prof'l Eng'rs v. United States*, 435 U.S. 679, 695 (1978) ("[U]ltimately competition will produce not only lower prices, but also better goods and services. The heart of our national economic policy long has been faith in the value of competition.") (internal quotations omitted). In drafting Section 230, Congress enshrined that free market principle in its express policy recitation. *See* 47 U.S.C. § 230(b)(2). Congress signaled that, although businesses should enjoy certain protections while operating on the Internet, it did not intend to broadly

alter, or exempt online businesses from, generally applicable rules outlawing anticompetitive behavior. As the Ninth Circuit cautioned in another case:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress [in Section 230] and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 n.15 (9th Cir. 2008) (en banc).

B. Malwarebytes' Attacks on the Ninth Circuit Opinion Have No Merit

Malwarebytes levies several unsupported attacks on the Ninth Circuit Opinion. ***First***, Malwarebytes accuses (at 5) the Ninth Circuit of relying on abstract policy and "ill-defined indicia of congressional intent," as though the Ninth Circuit had made policy declarations in a vacuum. To the contrary, the Ninth Circuit used the express policies spelled out in Section 230 to inform its understanding of the statutory text. Congress would not have included those express policies had it intended courts to ignore them or to interpret other portions of Section 230 to directly conflict with them. *See Gundy v. United States*, 139 S. Ct. 2116, 2127 (2019) (plurality) (holding that an express "state-

ment of purpose" "is an appropriate guide to the meaning of the statute's operative provisions") (alteration and internal quotations omitted), *reh'g denied*, 140 S. Ct. 579 (2019).

Second, Malwarebytes erroneously claims (at 11-12) that the Ninth Circuit applied a policy judgment to override otherwise clear and unambiguous statutory language. In fact, the Ninth Circuit adhered to foundational principles of statutory construction, interpreting the meaning of an undefined phrase, "otherwise objectionable," in a manner that effectuates statutory intent, gives effect to every part of the statute, and avoids absurd results. *See Parker Drilling Mgmt. Servs., Ltd. v. Newton*, 139 S. Ct. 1881, 1888 (2019) ("[T]he words of a statute must be read in their context and with a view to their place in the overall statutory scheme.") (internal quotations omitted).

Third, Malwarebytes suggests (at 13-14) that the Ninth Circuit Opinion announced a generalized good-faith requirement for Section 230(c)(2)(B). In so arguing, it cites no passage in the Ninth Circuit Opinion articulating such a requirement and makes no reference to the specific two-prong test set forth in the Opinion.[5]

Finally, Malwarebytes claims that Section 230 requires that it be granted ***unqualified*** immunity to block any material that it wants, at any time, for any reason, without needing any support for its decision and regardless of the harmful impact of that blocking on its users.[6] In effect, Malwarebytes contends that

---

[5] The *amicus* briefs suffer from the same defect. *See* EFF Br. 3-5; ESET Br. 5; Internet Ass'n Br. 20-21; TechFreedom Br. 5.

[6] In doing so, Malwarebytes avoids any mention of the practical effects of its position in a world where, as the Cybersecurity

Section 230(c)(2), a "[p]rotection for '***Good Samaritan***' blocking and screening of offensive material" (emphasis added), should be read to protect ***bad actors*** from having to answer for the legal consequences of their anticompetitive acts. It cites nothing to support that outlandish position.

In seeking to act with impunity, Malwarebytes ignores not only the express policies set forth in Section 230 but also Section 230(c)(2)'s specific text (which Malwarebytes itself concedes is central to proper statutory construction). Malwarebytes' unbounded reading of "otherwise objectionable," if adopted, would constitute a judicial rewrite of the actual statutory language of "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" to "material that the provider or user considers to be objectionable." That is, Malwarebytes asks the

---

Experts *amici* recognize (at 4), cyber threats can cause "massive economic harm and disruption." Malwarebytes' blocking—the functional equivalent of Apple programming its iPhones to disable competing Samsung smartphones in the same household—sets a dangerous precedent. It opens the door to every cybersecurity company blocking and disabling the programs of every one of its competitors. This is not merely hypothetical—ESET, LLC, a competitor of both Malwarebytes and Enigma, has filed a self-interested *amicus* brief in support of an unbridled test that would allow it to unfairly target competitors. In such a world, cybersecurity companies would focus more on fighting each other than on combatting cyber threats, and the variety and quality of cybersecurity products would suffer. Larger technology companies would be free to unlawfully block programs from smaller technology companies, squeezing those companies out of the market, stifling competition, and reducing consumer choice. At a minimum, consumers would be less safe from cyber threats because they would be able to run only one company's program, when industry best practices suggest running several programs simultaneously for multiple layers of cybersecurity protection.

Court to erase nine full words from the statute, violating the core principle of text-based statutory construction that each word of a statute be given effect. *See*, *e.g.*, *Obduskey v. McCarthy & Holthus LLP*, 139 S. Ct. 1029, 1037 (2019) ("[W]e generally presum[e] that statutes do not contain surplusage.") (internal quotations omitted) (first alteration added).

II. THERE IS NO CONFLICT WARRANTING THE COURT'S REVIEW

The Ninth Circuit's decision does not conflict with a decision by any other federal court of appeals or state court of last resort. In fact, this case is one of first impression on whether Section 230(c)(2)(B) immunizes a software provider's blocking of a direct competitor for anticompetitive purposes. *See* Pet. App. 19a. The best Malwarebytes can do is to assert illusory generalized conflicts.

A. Malwarebytes' Claim of a Generalized Circuit Conflict Is Baseless

Absent a direct Circuit conflict, Malwarebytes claims (at 5) a generalized conflict with "prevailing" broad judicial interpretations of Section 230 immunity. No such conflict exists. The Ninth Circuit Opinion agrees that Section 230 confers broad immunity; it clarifies only that the immunity is not "unfettered" and cannot extend so far as predatory anticompetitive targeting of a direct competitor. Pet. App. 6a, 11a. Malwarebytes cites ***no*** case declaring Section 230 immunity to be unlimited. Moreover, every case Malwarebytes does cite (at 17-18) as requiring an "expansive[]" reading of Section 230(c)(2) concerns the other subsection of Section 230, Section 230(c)(1), which has a much different text, structure, function,

and origin, and covers a different category of defendants and behaviors.[7]

Malwarebytes also attempts to manufacture a conflict with *Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010), as to the proper method for statutory construction. In *Comcast*, the D.C. Circuit considered Section 230 in an entirely different context than the Ninth Circuit Opinion. Specifically, the D.C. Circuit

---

[7] *See Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008) ("Section 230(c)(1) is general."); *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016) ("courts have invoked the prophylaxis of section 230(c)(1) in connection with a wide variety of causes of action"); *Force v. Facebook, Inc.*, 934 F.3d 53, 64 (2d Cir. 2019) ("[T]he Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity."), *cert. denied*, No. 19-859 (U.S. May 18, 2020); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (discussing the immunity conferred by Section 230(c)(1), "[t]he relevant portion" of Section 230); *Hassell v. Bird*, 420 P.3d 776, 791 (Cal. 2018) (plurality op.) (opining on the interface between Section 230(c)(1) and Section 230(e)(3)), *cert. denied*, 139 S. Ct. 940 (2019); *Shiamili v. Real Estate Grp. of N.Y., Inc.*, 952 N.E.2d 1011, 1017 (N.Y. 2011) (holding that Section 230(c)(2) "bar[s] lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content") (internal quotations omitted); *Doe v. MySpace, Inc.*, 528 F.3d 413, 422 (5th Cir. 2008) ("[b]ecause we affirm the district court based upon the application of § 230(c)(1), there is no need to apply § 230(c)(2)"); *Johnson v. Arden*, 614 F.3d 785, 792 (8th Cir. 2010) ("the Johnsons' claims against InMotion fail as a matter of law under § 230(c)(1)"); *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321-22 (11th Cir. 2006) (considering claim based on Amazon publishing an author's image, an action covered by Section 230(c)(1), and citing *Zeran*, a case decided under Section 230(c)(1), in support of its point about "broad" immunity); *Marshall's Locksmith Serv. Inc. v. Google, LLC*, 925 F.3d 1263, 1267 (D.C. Cir. 2019) ("[t]o determine whether dismissal is appropriate, this circuit has adopted a three-pronged test that tracks the text of § 230(c)(1)").

rejected a federal agency's claim of "authority to regulate an Internet service provider's network management practices" under the Communications Act of 1934, because the statutory text did not grant "express statutory authority over such practices" to the agency and Section 230's "statements of policy, by themselves, do not create statutorily mandated responsibilities." *Id.* at 644 (internal quotations omitted). *Comcast* thus does not address whether an entity blocking a direct competitor under Section 230(c)(2) is entitled to immunity. The Ninth Circuit Opinion, in turn, does not implicate the regulatory authority assessed by the *Comcast* court, which entailed a particularized application of a test for "ancillary jurisdiction" under the Federal Communications Commission's regulations. *Id.* at 646.

To the extent *Comcast* can even be said to declare a general rule of statutory construction applicable to Section 230(c)(2), the Ninth Circuit Opinion does not contradict such a rule. The Ninth Circuit does not rely on "statements of policy" to justify the creation of new "responsibilities" absent from the statute. Rather, the Ninth Circuit considered the express policies Congress set forth in Section 230 to inform its interpretation of the statutorily undefined and disputed term "otherwise objectionable." *See* Pet. App. 19a.

Finally, Malwarebytes erroneously claims (at 19-20) a conflict between the Ninth Circuit Opinion and *Prager University v. Google LLC*, No. 19CV340667, 2019 WL 8640569 (Cal. Super. Ct., Santa Clara Cty., Nov. 19, 2019), *appeal docketed*, No. H047714 (Cal. Ct. App. 6th Dist. Dec. 19, 2019). *Prager*, a trial court decision currently on appeal to California's intermediate appellate court, is far from being final, binding law from California's state court of last resort.

Additionally, the Ninth Circuit Opinion would not be applicable to the fact pattern presented in *Prager*. In *Prager*, the California trial court opined on the restrictions placed by YouTube, a Google-owned "social media and video sharing platform," on content created by Prager University, "a non-profit . . . educational organization that promotes discussion on historical, religious, and current events by disseminating educational videos." *Id.* at *1. Prager University is not a direct competitor of YouTube in the "social media and video sharing platform" industry, and the case does not involve any alleged blocking by YouTube of competing video streaming platforms, like Vimeo. As a result, the Ninth Circuit Opinion's holding—that Section 230(c)(2) does not immunize blocking a direct competitor for anticompetitive purposes—has no bearing on *Prager*.[8]

B. The Decision Below Created No Intra-Circuit Conflict

The Ninth Circuit Opinion is fully consistent with the leading case on Section 230(c)(2), *Zango v. Kaspersky*. As the court explained, *Zango* "recognized that [Section 230(c)(2)] establishes a subjective standard whereby internet users and software providers decide what online material is objectionable," but

[8] The trial court's holding in *Prager* immunizing YouTube's restrictions on Prager University's content is entirely consistent with the relevant Ninth Circuit precedent. *Prager* itself states that its approach to Section 230(c)(1) "has been endorsed by the Ninth Circuit." 2019 WL 8640569, at *8. And *Zango*, like *Prager*, immunizes a provider of interactive computer services when it makes available to users the technical means to restrict access to material by a third-party non-competitor that the provider or user subjectively considers to be "obscene" or "excessively violent." *See id.* at *10; *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1177-78 (9th Cir. 2009).

"did not hold . . . that the immunity [conferred by that Section] was limitless." Pet. App. 5a-6a.

Zango specifically held that Section 230(c)(2) immunized Kaspersky's anti-virus software blocking Zango's programs as "adware, a type of malware." 568 F.3d at 1171. *Zango*, however, made no holdings implicating the direct competitor blocking issue in this case. Kaspersky and Zango were not direct competitors, unlike Enigma and Malwarebytes. *See* Pet. App. 6a. Moreover, "[t]he majority in *Zango* did not . . . address whether there were limitations on a provider's discretion to declare online content 'objectionable,'" because "[n]o such issue was raised in the appeal." *Id.* at 16a; *see also Zango*, 568 F.3d at 1177 n.8 ("Because Zango has not argued that the statute limits the material a provider of an interactive computer service may properly consider 'objectionable,' that question is not before us."); *id.* at 1178 (Fisher, J., concurring) (identifying Zango's waiver of any argument on appeal that its "software is not 'otherwise objectionable'").

In fact, Judge Fisher's *Zango* concurrence correctly identified as a matter for future resolution the precise issue in this case:

> [E]xtending immunity beyond the facts of this case could pose serious problems if providers of blocking software were to be given free license to *unilaterally* block the dissemination of material . . . .
>
> . . . [A] blocking software provider might abuse [Section 230(c)(2)(B)] immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material "otherwise objectionable." Focusing for the moment on anticompetitive

> blocking, I am concerned that blocking software providers who flout users' choices by blocking competitors' content could hide behind § 230(c)(2)(B) when the competitor seeks to recover damages. I doubt Congress intended § 230(c)(2)(B) to be so forgiving.

568 F.3d at 1178 (Fisher, J., concurring); *see also* Pet. App. 16a-17a ("It was Judge Fisher's concurring opinion in *Zango* that framed the issue for future litigation as to whether the term 'objectionable' might be construed in a way that would immunize providers even if they blocked online content for improper reasons.").

III. THE NINTH CIRCUIT'S NARROW AND FACT-BOUND DECISION IS NOT OF SUFFICIENT IMPORTANCE TO WARRANT REVIEW

The Ninth Circuit Opinion's applicability is limited to a subsection of Section 230, a small number of entities, and a narrow set of facts. Malwarebytes' contrary arguments misread the Ninth Circuit's holding and posit unrealistic slippery-slope hypotheticals.

First, Section 230(c)(2)(B)—the sole provision the Ninth Circuit Opinion applied—extends only to a narrow group of "interactive computer service[s]" when they are taking "action . . . to enable or make available to information content providers or others the technical means to restrict access" to certain material. That section covers fewer entities than its counterpart Section 230(c)(2)(A), which applies more broadly to any "provider or user of an interactive computer service provider" that takes action to restrict access to that material. And, even combined, both prongs of Section 230(c)(2) have less reach and

are less frequently invoked than Section 230(c)(1), which protects any "provider or user of an interactive computer service" provider from being "treated as the publisher or speaker of any information provided by" someone else.

Second, the Ninth Circuit Opinion impacts only a subset of the already limited number of "interactive computer services" offering blocking or filtering software—the even smaller number of such companies that have shown an inclination to predatory behavior against a direct competitor. Neither Malwarebytes nor its *amici* demonstrate any pattern of companies blocking competitors under Section 230's protection that might warrant this Court's attention.

Third, for the narrow band of potential parties to whom the Ninth Circuit Opinion might be relevant, the Ninth Circuit announced a clear and specific two-prong test. It allows a plaintiff to overcome a Section 230(c)(2)(B) defense on a motion to dismiss only if the plaintiff can plausibly allege ***both*** (i) that it is a "competitor" of the defendant ***and*** (ii) that the defendant blocked plaintiff's material for "anticompetitive reasons." Pet. App. 23a. That two-prong test responds directly to the unique and egregious factual circumstances pleaded by Enigma: Malwarebytes' anticompetitive retaliation against Enigma's attempt to protect itself as a competitor.[9]

---

[9] Notably, Malwarebytes and its *amici* avoid discussing those facts, and instead reach well outside the record to make generalized arguments about irrelevant circumstances. If matters outside the record are to be considered, AV-Test is a highly respected independent testing lab whose malware research is cited by the Cybersecurity Experts *amici* (at 4) as evidence of the importance of anti-malware software. In 2017, AV-Test compared SpyHunter 4 and MBAM, and it determined that Enigma's program outperformed Malwarebytes' on both malware

Indeed, Malwarebytes itself sought and obtained confirmation from the Ninth Circuit of the narrowness of the holding. In its rehearing petition, Malwarebytes took issue with one sentence of the Ninth Circuit Opinion that it claimed might be read as adopting a looser standard, and, in response, the Ninth Circuit panel revised that sentence.[10] Letting the decision stand, therefore, would not result in a loss of immunity for defendants. For instance, Malwarebytes' claim (at 25) that malware or adware purveyors might plead around Section 230 posits only that those purveyors could try to claim they are competitors of anti-malware providers, by adding certain software features.[11] But direct competition is only the first

---

detection and remediation, thereby disproving any suggestion by Malwarebytes or *amici* that SpyHunter 4 is a "rogue" product. *See* AV-Test, *Comparative Remediation Testing Report* (May 2017), https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Enigma_Comparative_Remediation_Testing_Report_May_2017_EN.pdf. Malwarebytes' continued designation of SpyHunter 4 as a PUP and threat demonstrates its malicious intent and pretextual explanation for the blocking.

[10] The original sentence read: "What is clear to us from the statutory language, history and case law is that the criteria for blocking online material must be based on the characteristics of the online material, *i.e.* its content, and not on the identity of the entity that produced it." Pet. App. 39a. The revised sentence states: "What is clear to us from the statutory language, history, and case law is that providers do not have unfettered discretion to declare online content 'objectionable' and blocking and filtering decisions that are driven by anticompetitive animus are not entitled to immunity under section 230(c)(2)." *Id.* at 11a.

[11] Malwarebytes' concern—echoed by ESET (at 6-7)—also rests on the faulty assumption that district courts will not be able to see through such a transparent ploy and act accordingly. As discussed *infra*, district courts have both ample experience in evaluating and rejecting such claims, and the appropriate procedural mechanisms to do so expeditiously.

prong of the Ninth Circuit's test, and Malwarebytes nowhere demonstrates how malware purveyors might allege malicious and obvious anticompetitive targeting of the kind Malwarebytes perpetrated against Enigma. For that same reason, "automated algorithms" (Pet. 27) are not threatened by the Ninth Circuit opinion; those listed as a result of such algorithms (if competitors) might be able to plead anticompetitive ***effects***, but could not satisfy the higher burden of alleging specific anticompetitive ***targeting***.[12]

Fourth, the filtering tools Malwarebytes cites (at 29-30) are not threatened by the Ninth Circuit Opinion. The content providers blocked by the Facebook "hide post" tool, the Twitter low-quality filter, Reddit's community editing, or YouTube's restricted mode are not direct competitors of Facebook, Twitter, Reddit, or YouTube. By extension, Malwarebytes' referenced entity "restrict[ing] . . . content in order to favor some competing content" (at 32) selects between the content

---

[12] *Amici*'s arguments suffer from similar defects. EFF, for instance, expresses concern (at 7-8) regarding "false positives," but does not explain how a "false positive" block would support pleading the required selective targeting. It also ignores the reality of how a "false positive" block would be handled in the industry. Companies faced with a block in the first instance reach out to the blocker to seek an amicable resolution; if the block was the result of a "false positive" algorithm detection, the provider of the blocking software, once notified, simply removes the block. The vast majority of blocks are resolved this way, without any involvement from the courts. Conversely, if a block is not a false positive but rather is intentional because the blocked "anti-threat software" is a "genuine threat," Cybersecurity Experts *amici* (at 5-7) fail to explain how the plaintiff will make specific allegations of anticompetitive targeting. Moreover, even if a plaintiff could make such allegations, the defendant still would have ample opportunity under the Ninth Circuit standard to establish that its blocking is justified.

of two competing third parties, rather than restricting access to its own competitor's product. Moreover, the content provider—an individual user—could not plausibly allege Facebook, Twitter, Reddit, or YouTube specifically targeted that user when each service has millions of users. And Malwarebytes entirely ignores that much of the content blocked by those tools qualifies as "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing," rendering the blocking firmly immunized by Section 230 regardless of how the limits of "otherwise objectionable" are interpreted.[13]

Fifth, a tsunami of litigation will not ensue as a result of the Ninth Circuit Opinion. District courts are well equipped to assess the plausibility of pleadings at the motion-to-dismiss stage under the *Twombly/*

---

[13] *Amici* Internet Association (at 14-17) and TechFreedom (at 14-15) make the same erroneous claims about those and other filtering tools. *Amicus* EFF also voices concerns (at 12-14) about certain filtering tools. In the case of Privacy Badger, EFF struggles to explain how a challenger could even allege it competes with EFF. Moreover, EFF explains that Privacy Badger adds material to a block list based on automated heuristics, and it does not attempt to posit how a challenger would spin that scenario to allege specific anticompetitive targeting like that pled in this case. EFF's purported worry regarding anti-spyware tools provided by anti-virus vendors is even less credible. The creators of spyware, however creative, could not plausibly allege that they are direct competitors of Kaspersky Lab, let alone allege specific anticompetitive targeting. EFF's reference (at 14) to potential allegations by spyware vendors that their software is legitimate is a red herring. Nowhere did the Ninth Circuit hold that such a bald allegation of legitimacy would be sufficient under its two-prong test (as evidenced by EFF's lack of citation to the Opinion). Enigma, as set forth *supra* in the Statement, pleaded substantially more, and with far greater specifics.

Iqbal[14] standard, as they have done for years.[15] As the Cybersecurity Experts *amici* (at 15) themselves acknowledge, the Northern District of California recently dismissed a lawsuit against Malwarebytes brought by a provider of a different kind of software, on the grounds that the plaintiff did not plausibly allege that the parties were direct competitors under the Ninth Circuit Opinion's test. *See Asurvio LP v. Malwarebytes Inc.*, No. 5:18-cv-05409-EJD, 2020 WL 1478345 (N.D. Cal. Mar. 26, 2020).[16] *Asurvio* demonstrates that the Ninth Circuit Opinion provides district courts adequate guidance on how to apply its test.[17]

---

[14] *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

[15] To the extent *amicus* EFF intends to suggest (at 6) that Section 230(e)(3) prevents lawsuits from being brought at all, as an initial matter Malwarebytes did not invoke that section and thus has waived the argument. In any event, Section 230(e)(3) does no such thing. Using classic preemption and savings language, it merely provides that state-law claims may be enforced if consistent with Section 230 but are preempted if inconsistent. *See generally Wyeth v. Levine*, 555 U.S. 555 (2009). Here, the Ninth Circuit held that Section 230 does not apply to entities blocking direct competitors for anticompetitive purposes, and Section 230(e)(3) therefore permits the enforcement of state-law claims against such behavior.

[16] Malwarebytes' petition does not mention this decision.

[17] In earlier cases, district courts had applied narrower constructions of "otherwise objectionable" than that of the Ninth Circuit Opinion without conceptual difficulty and without any resulting spike in numbers of lawsuits filed. *See*, *e.g.*, *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883-84 (N.D. Cal. 2015) (rejecting "reading 'otherwise objectionable' to mean anything to which a content provider objects regardless of why it is objectionable" and instead applying *ejusdem generis* to cabin "otherwise

Finally, Malwarebytes makes (at 31-32) a series of internally inconsistent arguments about the impact of the Ninth Circuit Opinion on the other more widely applicable parts of Section 230. Malwarebytes claims the Ninth Circuit Opinion will somehow *restrict* immunity under Section 230(c)(2)(A), even though it highlights that subparagraph (A) already includes an express "good faith" requirement and argues (at 13-14) that the Ninth Circuit's test is supposedly coterminous with that "good faith" requirement. Malwarebytes also vaguely refers to the possibility of courts applying the Ninth Circuit's holding to Section 230(c)(1), even though the holding is specific to the ***blocking*** of content, and Malwarebytes itself specifies (at 33) that subsection (c)(1) is about "the decision to ***leave up*** third-party content" (emphasis added). Malwarebytes' far-fetched musings should not distract the Court from the fact that the Ninth Circuit's holding is ultimately very limited and narrowly applicable, rendering review by this Court unnecessary.

---

objectionable" by "the list preceding" it of "obscene, lewd, lascivious, filthy, excessively violent, [and] harassing" material); *Nat'l Numismatic Certification, LLC v. eBay, Inc.*, No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *25 (M.D. Fla. July 8, 2008) (rejecting the argument "that Congress intended the general term 'objectionable' to [immunize restricting access to] an auction of potentially-counterfeit coins" because "the word ['objectionable'] is preceded by seven other words that describe pornography, graphic violence, obscenity, and harassment"); *Goddard v. Google, Inc.*, No. C 08-2738 JF (PVT), 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008) (adopting the reasoning of *National Numismatic Certification* on this point); *Sherman v. Yahoo! Inc.*, 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014) ("The Court declines to broadly interpret 'otherwise objectionable' material to include any or all information or content.").

IV. THIS CASE IS A POOR VEHICLE FOR FURTHER REVIEW

Even if the Court were inclined to review the appropriate scope of Section 230(c)(2), this case is a poor vehicle for doing so for three reasons.

First, the case below is not final. The Ninth Circuit Opinion rules only on the adequacy of Enigma's allegations on a Rule 12(b)(6) motion to dismiss, allowing Enigma to proceed to discovery. Malwarebytes can renew its argument that Section 230(c)(2) should immunize blocking direct competitors for anticompetitive purposes at summary judgment or trial. Review at that point would enable the Court to assess the issues on a complete factual record.

Second, the Ninth Circuit made a very specific and narrow ruling—that Section 230(c)(2) does not immunize blocking a direct competitor for anticompetitive purposes. That ruling stemmed from unique factual circumstances far afield from the typical Section 230(c)(2) dispute, *i.e.*, that Malwarebytes intentionally targeted a direct competitor for specific anticompetitive purposes, including to directly retaliate for Enigma's prosecution of the Related Case and service of the Subpoena. Those facts do not lend themselves to a broader statutory review by this Court.

Finally, substantial recent activity in both the legislative and executive branches of the federal government in connection with potential revisions of Section 230 suggests that this Court should not undertake a review of Section 230 at this time. Section 230 has already been amended once recently with overwhelming bipartisan support, through 2018's Allow States and Victims to Fight Online Sex Trafficking

Act (FOSTA).[18] Multiple congressional bills proposing further amendments to Section 230, several of which have bipartisan support, have been introduced since the start of 2019.[19] Malwarebytes itself recognizes (at 34) that a number of "[p]rominent" Senators are currently focused on Section 230. Moreover, in the spring of 2020, the Department of Justice also undertook a Section 230 review, and in June 2020 issued recommendations for the provision's reform.[20] Developments

---

[18] *See* Pub. L. No. 115-164, 132 Stat. 1253; http://clerk.house.gov/evs/2018/roll091.xml (House 388-25 vote in favor); https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=115&session=2&vote=00060 (Senate 97-2 vote in favor). *Amicus* EFF points (at 8-10) to FOSTA as reason to be wary of exceptions to Section 230 immunity, but the specifics of the FOSTA amendment render that caution irrelevant here. FOSTA amended Section 230(e) in a manner that impacted Section 230(c)(1), not the subsection on which the Ninth Circuit ruled, and had far broader reach than the narrow, common-sense limitation recognized in the Ninth Circuit Opinion.

[19] *See* "Biased Algorithm Deterrence Act of 2019," H.R. 492, 116th Cong. (2019) (introduced Jan. 11, 2019; sponsored by Rep. Gohmert (R-TX)); "Ending Support for Internet Censorship Act," S. 1914, 116th Cong. (2019) (introduced June 19, 2019; sponsored by Sen. Hawley (R-MO)); "Stop the Censorship Act," H.R. 4027, 116th Cong. (2019) (introduced July 25, 2019; sponsored by Rep. Gosar (R-AZ)); "EARN IT Act of 2020," S. 3398, 116th Cong. (2020) (introduced Mar. 5, 2020; sponsored by Sen. Graham (R-SC), with 4 Republican and 6 Democratic co-sponsors); "Limiting Section 230 Immunity to Good Samaritans Act," S. 3983, 116th Cong. (2020) (introduced June 17, 2020; sponsored by Sen. Hawley (R-MO)); "Platform Accountability and Consumer Transparency Act (PACT Act)," S. 4066, 116th Cong. (2020) (introduced June 24, 2020; sponsored by Sens. Schatz (D-HI) and Thune (R-SD)).

[20] *See* U.S. Dep't of Justice, Office of Att'y Gen., Department of Justice's Review of Section 230 of the Communications Decency Act of 1996, https://www.justice.gov/ag/department-

from the federal legislature and executive branch may well moot any rulings this Court would issue in reviewing the Ninth Circuit Opinion.[21]

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted,

CHRISTOPHER M. VERDINI
ANNA SHABALOV
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
(412) 355-6500

TERRY BUDD
Counsel of Record
BUDD LAW, PLLC
120 Lyndhurst Circle
Wexford, PA 15090
(412) 613-2541
(terry.budd@buddlawglobal.com)

July 27, 2020

---

justice-s-review-section-230-communications-decency-act-1996 (last visited July 23, 2020); U.S. Dep't of Justice, *Section 230 — Nurturing Innovation or Fostering Unaccountability?: Key Takeaways and Recommendations* (June 2020), https://www.justice.gov/file/1286331/download.

[21] On May 28, 2020, President Trump issued an Executive Order titled "Preventing Online Censorship" that sets forth an interpretation of Section 230 and requests various related actions from federal agencies. *See* Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (May 28, 2020). The Executive Order has no bearing on this case, and challenges to it implicate different legal concerns. *See*, *e.g.*, Compl., *Ctr. for Democracy & Tech. v. Trump*, No. 1:20-cv-01456, Dkt. 1 (D.D.C. June 2, 2020) (challenging the Executive Order as an *ultra vires* action in violation of the First Amendment). Should the Court be interested in reviewing any aspect of the Executive Order, it will have ample opportunity to do so in due course through direct challenges to that Order.