No. 19-

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

PETITION FOR A WRIT OF CERTIORARI

TYLER GRIFFIN NEWBY
FENWICK & WEST LLP
555 California Street
12th Floor
San Francisco, CA 94104

NEAL KUMAR KATYAL
Counsel of Record
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth St., N.W.
Washington, D.C. 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

QUESTION PRESENTED

Section 230(c)(2)(B) of the Communications Decency Act provides immunity from most civil liability to computer-service providers for "any action taken to enable or make available to * * * others the technical means to restrict access to material" that "the provider or user considers to be * * * objectionable." 47 U.S.C. § 230(c)(2). The court below agreed that none of the narrow, express exceptions to that immunity in Section 230(e) apply here. The question presented is:

Whether federal courts can derive an implied exception to Section 230(c)(2)(B) immunity for blocking or filtering decisions when they are alleged to be "driven by anticompetitive animus."

PARTIES TO THE PROCEEDING

Malwarebytes, Inc., petitioner on review, was the defendant-appellee below.

Enigma Software Group USA, LLC, respondent on review, was the plaintiff-appellant below.

RULE 29.6 DISCLOSURE STATEMENT

Malwarebytes, Inc. has no parent corporation, and no publicly held company owns 10% or more of its stock.

RELATED PROCEEDINGS

U.S. Court of Appeals for the Ninth Circuit:

Enigma Software Group USA, LLC v. *Malwarebytes, Inc.*, No. 17-17351 (9th Cir. Dec. 31, 2019) (reported at 946 F.3d 1040)

Enigma Software Group USA, LLC v. *Malwarebytes, Inc.*, No. 17-17351 (9th Cir. Sep. 12, 2019) (reported at 938 F.3d 1026) (opinion withdrawn and superseded on denial of rehearing)

U.S. District Court for the Northern District of California:

Enigma Software Group USA LLC v. *Malwarebytes Inc.*, No. 5:17-cv-02915-EJD (N.D. Cal. Nov. 7, 2017) (unreported)

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

Page(s)

CASES:

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

STATUTES:

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES:

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

IN THE
Supreme Court of the United States

No. 19-

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

PETITION FOR A WRIT OF CERTIORARI

Malwarebytes, Inc., respectfully petitions for a writ of certiorari to review the judgment of the Ninth Circuit in this case.

OPINIONS BELOW

The Ninth Circuit's amended opinion, issued on denial of rehearing, is reported at 946 F.3d 1040. Pet. App. 1a-29a. Its original, superseded opinion is reported at 938 F.3d 1026. Pet. App. 30a-56a. The district court's order granting Malwarebytes's motion to dismiss is unreported. *Id.* at 57a-65a.

JURISDICTION

The Ninth Circuit entered judgment on September 12, 2019. Pet. App. 1a, 30a. Malwarebytes timely

petitioned for panel rehearing and rehearing en banc, which were denied on December 31, 2019. *Id.* at 1a, 4a-5a. Justice Kagan extended the time to file a petition for certiorari to May 11, 2020. This Court's jurisdiction rests on 28 U.S.C. § 1254(1).

STATUTORY PROVISIONS INVOLVED

Section 230(c)(2) of the Communications Decency Act, 47 U.S.C. § 230(c)(2), provides that:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

The entirety of Section 230 is reproduced in the appendix to this petition, Pet. App. 66a-71a, as is the text of Section 230 as it appeared before its 2018 amendments, *id.* at 72a-76a.

INTRODUCTION

The Communications Decency Act (CDA) is foundational to the Internet as we know it. Faced with a revolutionary new technology, Congress chose a system of self-regulation—one that would leave users, rather than governments or courts, in control

of their own experience. The cornerstone of that system is the immunity from civil liability provided in Section 230(c). Through that provision, Congress ensured that Internet providers and users would be free from the constant threat of litigation for moderating threatening or objectionable content. Of course, that would be impossible without adequate tools for screening and filtering content. Thus, in Section 230(c)(2)(B), Congress extended that immunity—without qualification—to providers for "any action taken to enable or make available" the "technical means to restrict access to" content the provider "considers to be" objectionable. 47 U.S.C. § 230(c)(2).

Petitioner Malwarebytes, Inc., is a leading software security firm that provides filtering tools to consumers. Its software flags security threats and other unwanted programs, and asks users whether they wish to retain those programs. After an update to Malwarebytes's software began flagging Respondent's products as potentially unwanted programs and providing its users the choice to use or to quarantine the products, Respondent sued Malwarebytes. The plain text of the Act forbids exactly this kind of retaliatory suit.

In the decision below, however, a divided panel of the Ninth Circuit read the Act to contain an implied exception for actions allegedly motivated by "anti-competitive animus." To its credit, the court did not even try to justify that reading based on the text of the statute. Instead, the court relied exclusively on its own mistaken understanding of the policy interests at stake.

This Court's precedents flatly forbid that approach. In recent decades, this Court has instructed lower courts that statutory interpretation must be guided, first and foremost, by the text, and that even compelling policy considerations cannot justify an interpretation that runs counter to the text. The decision below defies that cardinal rule. It is therefore no surprise that—in both its reasoning and holding—the decision breaks from decisions of numerous other courts. And the conflict has only gotten worse in the short time since the court issued its decision, as a California state court has already issued a decision expressly disagreeing with it—opening a rift between state and federal fora in the technology center of the Nation.

It is critically important for the Court to correct the Ninth Circuit's erroneous interpretation now. By exposing developers of filtering tools to a flood of retaliatory litigation, the decision will have the opposite effect from Congress's goal of promoting development of such tools. Making matters worse, because the Ninth Circuit relied solely on policy considerations that apply to all of Section 230, its decision threatens *all* of Section 230(c)'s immunities. It is an open invitation for lower courts to allow a lawsuit anytime judges have their own policy concerns about a particular filtering decision or tool. The decision below thus risks exposing cybersecurity firms, as well as the most popular Internet services, to a raft of burdensome litigation for providing the filtering tools and exercising the content-moderation and editorial discretion that Congress sought to encourage. The result will be an Internet with less

consumer choice and less protection for users from offensive and objectionable content.

The decision below is a throwback to "a bygone era of statutory construction," when judges looked primarily to ill-defined indicia of congressional intent rather than statutory text. *Food Mktg. Inst.* v. *Argus Leader Media*, 139 S. Ct. 2356, 2364 (2019) (internal quotation marks omitted). The Court should grant certiorari to correct the Ninth Circuit's "casual disregard of the rules of statutory interpretation" and bring it back in line with the prevailing interpretations of Section 230. *Id.*

The petition should be granted.

STATEMENT

A. Statutory Background

The CDA emerged in 1996 as a response to the proliferation of offensive content on the nascent Internet. Congress sought an innovative approach for this new technology, one that would let "Government * * * get out of the way and let parents and individuals" "tailor what [they] see to [their] own tastes." 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox). The resulting Act therefore aimed "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 "to remove disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b)(3), (4).

Congress identified the threat of litigation as a particular obstacle to the development of "blocking and filtering technologies." *See* Pet. App. 8a-10a.

Early state-court decisions had made it challenging for Internet-based firms to take action against offensive or dangerous content by exposing those who did to liability. *See id.* (discussing *Stratton Oakmont, Inc.* v. *Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995)).

The operative text of the CDA took a three-pronged approach to eliminating the threat of such litigation.

First, in subsection (c)(1), Congress addressed immunity for hosting third-party content. It ensured that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). That provision bars suits seeking to hold providers liable for exercising "a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content." *Zeran* v. *Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

Second, in subsection (c)(2)(A), Congress provided immunity for those who block or filter content. Specifically, it barred civil liability against "provider[s]" and "user[s] of an interactive computer service" who take action "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." 47 U.S.C. § 230(c)(2)(A). That immunity is available for "any action," so long as it is "voluntarily taken in good faith." *Id.*

Third—and most relevant here—in subsection (c)(2)(B), Congress extended immunity to entities that develop and provide the technology necessary

for filtering and blocking content. That immunity covers "any action taken to enable or make available * * * the technical means to restrict access to" the material described in subsection (c)(2)(A), [1] *id.* § 230(c)(2)(B)—that is, "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable," *id.* § 230(c)(2)(A). Unlike the immunity for those who themselves "*restrict* access to or availability of" such material, the immunity for developers of filtering technology is not conditioned on "good faith." *Compare id.* (emphasis added), *with id.* § 230(c)(2)(B).

Congress also provided a handful of exceptions to the CDA's immunity, including with respect to intellectual property laws and communications privacy laws. *See, e.g.*, *id.* § 230(e)(2), (4). None of those exceptions refers to antitrust law or "anticompetitive" behavior. *See id.* § 230(e).

B. Procedural Background

1. Malwarebytes is an Internet security firm with an international customer base. Pet. App. 12a. Users download its software to protect themselves from a wide array of threats on the Internet. These include "malware," which can damage operating systems or steal user information, and "Potentially Unwanted Programs" (or "PUPs") that falsely de-

---

[1] As enacted, the text cross-references subsection (c)(1), *see* 47 U.S.C. § 230(c)(2)(B), but that is uniformly regarded as a scrivener's error, *see Zango, Inc.* v. *Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 n.5 (9th Cir. 2009).

ceive users into thinking something is wrong with their computer so that they will download paid products to combat the supposed threats. *See id.* When Malwarebytes's "software detects an unwanted program, it displays a notification and asks the user if she wants to remove the program from her computer." *Id.* at 58a. In other words, users make the final decision about what gets filtered.

In October 2016, Malwarebytes adopted new criteria for identifying a PUP. *Id.* at 12a-13a. Using those criteria, Malwarebytes's software began classifying certain products of Respondent Enigma Software Group as a PUP. *Id.* As with any PUP, Malwarebytes' software gave users the option to retain, quarantine, or remove Enigma's products. *Id.* at 12a-13a, 58a.

2. Enigma sued Malwarebytes, alleging state-law business torts and unfair advertising in violation of the Lanham Act. *Id.* at 58a-59a. Malwarebytes moved to dismiss, invoking Section 230(c)(2)(B)'s immunity for providers of filtering software. *Id.* at 14a. Enigma opposed the motion, claiming "that Malwarebytes blocked Enigma's programs for anticompetitive reasons" and that the CDA's immunity is unavailable under such circumstances. *Id.* at 19a.

The District Court granted Malwarebytes's motion. *Id.* at 65a. It held that "the plain language of the statute" requires only that "*the provider* or user consider[]" the filtered material "objectionable." *Id.* at 62a (quoting 47 U.S.C. § 230(c)(2)). Thus, it was irrelevant *why* Malwarebytes considered Enigma's products "objectionable." *See id.* The court noted that the neighboring provision addressing immunity

for those who actually "restrict access" to content "include[s] a good-faith requirement." *See id.* at 63a (discussing 47 U.S.C. § 230(c)(2)(A)). Because Congress "chose not to" "include[ ] a similar reference" to good faith in subsection (c)(2)(B), the court declined to find a similar exception implied there. *Id.*

3. A divided panel of the Ninth Circuit reversed. *Id.* at 27a. Looking to the "history and purpose" of the CDA, *id.* at 19a, the majority held that Section 230(c)(2)'s immunity provisions contain an unstated exception for "decisions that are driven by anticompetitive animus," *id.* at 11a. Although the court acknowledged that its reading was in tension with "the unwillingness of Congress to spell out the meaning of 'otherwise objectionable,'" it felt obliged to update the statute for "today" by reading it not "to give providers unbridled discretion to block online content." *Id.* at 20a. Although the court did not explain how its reading was compatible with the operative text of the statute or the ordinary meaning of the word "objectionable," it found support for its reading in "the statute's express policies." *Id.* at 20a-21a.[2]

Judge Rawlinson dissented. The majority's reading, she explained, "cannot be squared with the broad language of the Act." *Id.* at 29a. "Under the language of the statute, if the blocked content is

---

[2] Separately, the court rejected Enigma's argument that its Lanham Act false-advertising claim falls within the CDA's exception for "intellectual property" law. Pet. App. 23a-27a. Malwarebytes does not seek review of this issue.

'otherwise objectionable' to the provider, the Act bestows immunity." *Id.* (quoting *Zango*, 568 F.3d at 1173). "The majority's real complaint," the dissent pointed out, "is not that the district court construed the statute too broadly, but that the statute is written too broadly." *Id.* at 28a. Such an issue "is one beyond [judicial] authority to correct." *Id.*

Over Judge Rawlinson's dissent, the Ninth Circuit denied Malwarebytes's petition for rehearing and rehearing en banc. *Id.* at 4a-5a.[3] This timely petition followed.

REASONS FOR GRANTING THE PETITION

I. THE DECISION BELOW DEFIES THIS COURT'S BASIC RULES OF STATUTORY INTERPRETATION AND DEVIATES FROM COURTS' SETTLED UNDERSTANDINGS OF SECTION 230.

One of this Court's most fundamental precepts is that statutory interpretation must begin with the text—and end there when the text is clear. This Court has repeatedly granted certiorari to clarify that principle. *See, e.g.*, *Food Mktg. Inst.*, 139 S. Ct. at 2364 ("We cannot approve such a casual disregard of the rules of statutory interpretation.").

---

[3] The panel issued an amended opinion that modified a sentence suggesting that immunity would be unavailable *anytime* a decision was motivated by "the identity of the entity that produced" the filtered content. *Compare* Pet. App. 39a, *with id.* at 11a-12a. It made no other changes.

The Ninth Circuit flouted that rule in this case. The court never explained how its reading bears any relationship to the operative text of the statute. Instead, it relied exclusively on its own policy concerns (which were themselves questionable). Unsurprisingly, that fundamentally flawed approach led the court to the wrong outcome in this case.

Not only did the Ninth Circuit's approach defy this Court's precedent, it upended the widely-shared consensus among lower courts that Section 230's immunity provisions should be read broadly. The court also broke from the D.C. Circuit by using the CDA's prefatory statutory goals to override its operative text, and the resulting interpretation of subsection (c)(2)(B) has been flatly rejected by state courts in the very same State where this litigation arose, California. These conflicts on an issue of critical importance further counsel this Court's intervention.

A. The Decision Below Erroneously Relied On Policy Rather Than Text To Interpret Section 230.

1. "[I]n any statutory construction case," a court must "start, of course, with the statutory text." *Sebelius* v. *Cloer*, 569 U.S. 369, 376 (2013) (quoting *BP Am. Prod. Co.* v. *Burton*, 549 U.S. 84, 91 (2006)). This Court's cases insisting on that approach are legion. *See, e.g.*, *Barnhart* v. *Sigmon Coal Co.*, 534 U.S. 438, 461-462 (2002) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.").

"When the words of a statute are unambiguous, then, this first canon is also the last: judicial inquiry is complete." *Id.* at 462 (internal quotation marks omitted). A statute's text is not "ambiguous" merely because it uses "[b]road general language." *Diamond* v. *Chakrabarty*, 447 U.S. 303, 315 (1980). Only after examining "the text of the provision in question" and discerning a genuine ambiguity may a court "move on, as need be, to the structure and purpose of the Act in which it occurs." *N.Y. State Conference of Blue Cross & Blue Shield Plans* v. *Travelers Ins. Co.*, 514 U.S. 645, 655 (1995); *accord Food Mktg. Inst.*, 139 S. Ct. at 2364 (finding it "inappropriate[ ]" to "resort to legislative history before consulting [a] statute's text and structure"). Courts "[l]ack[ ] the expertise or authority to assess the[ ] important competing claims" involved in policy disputes, which are "best addressed to the Congress." *Dunn* v. *Commodity Futures Trading Comm'n*, 519 U.S. 465, 480 (1997). And, critically, "[p]olicy considerations cannot override [an] interpretation of the text and structure of [an] Act." *Cent. Bank of Denver, N.A.*, v. *First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 188 (1994).

2. The Ninth Circuit broke sharply from this method of statutory interpretation. It started with its view of the statute's "history and purpose," not text. Pet. App. 19a. Indeed, the court apparently recognized that its approach was *in*compatible with Section 230's text: It took note of Congress's "unwillingness * * * to spell out the meaning of 'otherwise objectionable,' " and acknowledged that the text confers a "broad grant of protective control" to Internet providers. *Id.* at 20a.

Although the court linked its reading of the statute to the word "objectionable," *id.* at 23a, that relationship was not based on the "ordinary * * * meaning" of the term, as this Court's cases require, *Wisconsin Cent. Ltd.* v. *United States*, 138 S. Ct. 2067, 2074 (2018) (internal quotation marks omitted). The Ninth Circuit did not, for example, consider a definition of the term, or examine its meaning in other contexts. Instead, the court relied exclusively on two judges' perspective of the underlying policy interests. Pet. App. 20a (expressing concern that "[u]sers would not reasonably anticipate providers blocking valuable online content"). In fact, the court properly *rejected* Enigma's only argument based on the meaning of the word "objectionable." *See id.* at 21a (refusing to apply *ejusdem generis* to narrow the meaning of "objectionable" given the "breadth of the term" and the lack of similarity among subsection (c)(2)'s "enumerated categories").

By reading an unstated exception into the Act, the Ninth Circuit ignored a tried-and-true canon of textual analysis. "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) (internal quotation marks and alteration omitted). Here, Congress included a "good faith" requirement to claim immunity under subsection (c)(2)(A). The absence of any similar language indicates the "intentional[ ] * * * exclusion" of any similar motive-based requirement for subsection (c)(2)(B)'s immunity.

Malwarebytes made this point in its appellate brief, Malwarebytes C.A. Answering Br. 29-30, and rehearing petition, C.A. Reh'g Pet. 11-12. Yet the panel majority failed to even acknowledge it.

The court's sole justification for bypassing all of these bedrock rules of construction was policy. Pet. App. 19a-21a. Under this Court's precedent, that is no justification at all. Courts have "no roving license, in even ordinary cases of statutory interpretation, to disregard clear language simply on the view that * * * Congress 'must have intended' something" else. *Michigan* v. *Bay Mills Indian Cmty.*, 572 U.S. 782, 794 (2014); *see also Romag Fasteners, Inc.* v. *Fossil Grp., Inc.*, __ S. Ct. __, slip op. at 7 (2020) ("[T]he place for reconciling competing and incommensurable policy goals * * * is before policymakers."). The Ninth Circuit suggested that its emphasis on policy might be justified by Congress's inclusion of policy statements in the CDA. *See* Pet. App. 11a, 20a-21a. Wrong again. Congressional findings are too "thin" a "reed upon which to base" an exception for "motive" that is "neither expressed nor * * * fairly implied in the operative sections of the Act." *Nat'l Org. for Women, Inc.* v. *Scheidler*, 510 U.S. 249, 260 (1994).

Making matters worse, the policy concern animating the majority was wholly unfounded. The panel feared that users would lose access to "valuable online content" because providers might "act for their own, and not the public, benefit." Pet. App. 20a. But Congress anticipated this very issue. This case concerns immunity under subsection (c)(2)(B), which applies only to entities that empower *others* to filter

content by supplying the "technical means" to do so. 47 U.S.C. § 230(c)(2)(B). The majority's concern is directed to those who "restrict access to or availability of material" under subsection (c)(2)(A), and that immunity is available only to those who act "in good faith." *Id.* § 230(c)(2)(A).[4] The majority's apparent confusion about this elementary issue only reinforces this Court's longstanding position that courts are "ill suited" "to make * * * policy judgments." *Perry* v. *Perez*, 565 U.S. 388, 393 (2012) (per curiam); *see also infra* pp. 21-29 (explaining why Malwarebytes's position better comports with Congress's stated policies to promote competition and user choice).

3. The Ninth Circuit's deeply flawed approach to statutory construction led it to an erroneous result. Under a plain-meaning analysis of Section 230's "broad language," Pet. App. 29a (Rawlinson, J., dissenting), Malwarebytes is entitled to immunity under subsection (c)(2)(B).

That provision immunizes (1) a "provider or user of an interactive computer service" that (2) offers to "others the technical means to restrict access to material" that (3) "the provider or user considers * * * harassing[ ] or otherwise objectionable." 47 U.S.C. § 230(c)(2). Only the third element was contested here, which makes sense: Malwarebytes's software is plainly an interactive computer service,

---

[4] Because Malwarebytes only claims immunity under subsection (c)(2)(B), Malwarebytes takes no position on whether the conduct alleged by Enigma in this case would fall short of the "good faith" required by subsection (c)(2)(A).

and it operates by giving users the "technical means," *id.* § 230(c)(2)(B), "to remove [a flagged] program from her computer," Pet. App. 58a.

That leaves only whether Enigma's products are "material that the provider" (here, Malwarebytes) "considers to be * * * objectionable." 47 U.S.C. § 230(c)(2)(A). Enigma's complaint answers that question in the affirmative by conceding that Malwarebytes considers Enigma's products "PUPs and 'threats.' " C.A. E.R. 24. Because the Act requires only that Malwarebytes "considers" the content to be "objectionable," that determination is sufficient for immunity to apply. The "ordinary, contemporary, common meaning," *Wisconsin Cent.*, 138 S. Ct. at 2074 (internal quotation marks omitted), of "objectionable" is easily capacious enough to encompass programs that Malwarebytes has deemed a "threat" or a "potentially unwanted program." *See, e.g.*, Webster's II New College Dictionary (1995 ed.) (defining "objectionable" as "[p]rovoking disapproval or opposition: offensive"); The American Heritage College Dictionary (3d ed. 1993) (similar definition). Section 230(c)'s caption reinforces that reading. *See Yates* v. *United States*, 574 U.S. 528, 539-540 (2015) (plurality op.). It clarifies the provision is meant to protect "blocking and screening of *offensive* material," even though the word "offensive" is not one of the enumerated categories in § 230(c)(2)'s list. 47 U.S.C. § 230(c) (emphasis added).

Because the Ninth Circuit only reached a contrary decision by disregarding this Court's rules for statutory interpretation, this Court's review is warranted. *See* Sup. Ct. R. 10(c). Allowing the decision below to

stand will embolden lower courts to carve out additional policy-driven exceptions to Congress's duly-enacted legislation. *See infra* pp. 31-35.

B. The Decision Below Splits From The Approach Of Numerous Other Courts.

Given how starkly the decision below deviates from this Court's precedents, it is no surprise that it renders the Ninth Circuit an outlier on Section 230 immunity.

1. Outside of the Ninth Circuit, courts are in agreement that Section 230's immunity provisions must be read expansively. As the Seventh Circuit has explained, that conclusion flows from Congress's choice to use broad language: "[T]he reason a legislature writes a general statute is to avoid any need to traipse through the United States Code" and state lawbooks to "consider all potential sources of liability, one at a time." *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc.* v. *Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008). Courts have widely honored that choice in the context of Section 230. *Jane Doe No. 1* v. *Backpage.com, LLC*, 817 F.3d 12, 18 (1st Cir. 2016) ("There has been near-universal agreement that section 230 should not be construed grudgingly."); *Force* v. *Facebook*, 934 F.3d 53, 64 (2d Cir. 2019) (noting "general agreement" that the CDA "should be construed broadly in favor of immunity"), *petition for cert. filed*, No. 19-859 (U.S. Jan. 2, 2020); *Zeran*, 129 F.3d at 331 (referring to "§ 230's broad immunity"); *Hassell* v. *Bird*, 420 P.3d 776, 788 (Cal. 2018) (plurality op.) ("the tools of statutory interpretation compel[ ] a broad construction of section 230"); *Shiamili* v. *Real Estate Grp. of N.Y., Inc.*, 952 N.E.2d

1011, 1016 (N.Y. 2011) ("Both state and federal courts around the country have generally interpreted Section 230 immunity broadly * * * ." (internal quotation marks omitted)); *accord Doe* v. *MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008); *Johnson* v. *Arden*, 614 F.3d 785, 791 (8th Cir. 2010); *Almeida* v. *Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006); *Marshall's Locksmith Serv. Inc.* v. *Google, LLC*, 925 F.3d 1263, 1267 (D.C. Cir. 2019).[5]

The decision below, however, takes the opposite approach. Motivated by policy concerns, it discerned "limitations in the scope of immunity" found nowhere in the Act's text. Pet. App. 18a. The Ninth Circuit therefore eschewed the broad reading of Section 230 adopted by other courts. And this is not the first time that the Ninth Circuit has resorted to policy arguments to give the CDA a narrow construction. *See Doe* v. *Internet Brands, Inc.*, 824 F.3d 846, 851-853 (9th Cir. 2016) (reading the Act to have a "narrow language and * * * purpose"). This decision cements the court's outlier status.

2. The decision below also places the Ninth Circuit in square conflict with the D.C. Circuit regarding the proper relationship of Section 230's express policy goals, *see* 47 U.S.C. § 230(b), with its operative text, *see id.* § 230(c)-(e). The panel repeatedly—and selectively—resorted to subsection (b)'s policy goals

[5] Although some of these decisions speak specifically in terms of subsection (c)(1), that merely reflects the facts of those cases. Nothing in the opinions' reasoning suggests the broad reading is limited to that subsection.

to justify its atextual approach to statutory construction. *See* Pet. App. 20a-21a (citing 47 U.S.C. § 230(b)(3), (4)).

The D.C. Circuit has rejected that analytical approach. In *Comcast Corp.* v. *Federal Communications Commission*, 600 F.3d 642 (D.C. Cir. 2010), the FCC argued that it possessed regulatory power over "an Internet service provider's network management practices." *Id.* at 644. Lacking any "express statutory authority over such practices," *id.*, the Commission turned to the policy goals enacted in subsection (b) of the CDA, claiming those goals could "anchor the exercise of [regulatory] authority" even without an express grant of power. *Id.* at 652. The D.C. Circuit rejected that argument, holding that "statements of policy, by themselves, do not create 'statutorily mandated responsibilities.' " *Id.* at 644. The alternative approach, the court explained, would "virtually free the Commission from its congressional tether." *Id.* at 655. The D.C. Circuit's approach is flatly at odds with Enigma's efforts to carve out an exception to the "statutorily mandated" immunity by relying on the CDA's "policy statements alone." *Id.* at 644, 654 (internal quotation marks omitted).

3. In near-record time, the Ninth Circuit's holding has provoked disagreement with a California state court. Just a few weeks after the panel issued its original decision, the California Superior Court issued an opinion "disagree[ing]" with the panel's approach, finding that it "ignore[d] the plain language of the statute by reading a good faith limitation into section 230(c)(2)(B)." *Prager Univ.* v. *Google LLC*, No. 19CV340667, 2019 WL 8640569, at *10

(Cal. Super. Ct. Nov. 19, 2019), *appeal docketed*, No. H047714 (Cal. Ct. App. Dec. 19, 2019). That holding led the court to reject a video-maker's claim that YouTube acted in bad faith by allowing users—such as parents, school administrators, or libraries—to enable a "Restricted Mode" that filters certain sensitive content, such as graphic violence and sexual material. *Id.* at *2, *4, *9-10.

Existing California precedent concerning Section 230 assures that decision will be affirmed. The California Court of Appeal has already held, in a different case, that "Section 230 imposes a subjective element into the [immunity] determination" by conferring immunity "so long as [the developer of the filter] *deemed* the material to be * * * objectionable." *Pallorium, Inc.* v. *Jared*, No. G036124, 2007 WL 80955, at *7 (Cal. Ct. App. Jan. 11, 2007) (emphasis added and internal quotation marks omtited). And that reading comports with the California Supreme Court's instruction to interpret Section 230 "literally" according to its text. *Barrett* v. *Rosenthal*, 146 P.3d 510, 529 (Cal. 2006). Thus, there is nothing to be gained by postponing consideration of the question presented. Delay would also be harmful given the high risk of forum shopping: Because California is located within the Ninth Circuit—and home to the Nation's hub of technological development—plaintiffs now have every incentive to bring suit in federal courts. Certiorari is necessary to eliminate that risk.

II. THE QUESTION PRESENTED IS OF SUBSTANTIAL IMPORTANCE.

Even if the CDA's text left any ambiguity to be resolved by reference to policy, the Ninth Circuit

profoundly misunderstood how those considerations apply to this case. In fact, the decision below undermines Congress's stated goals in enacting the CDA. It is therefore vital for the Court to address the question presented now. Otherwise, this interpretation will fester—and in the circuit where Section 230 matters the most.

Congress's central goal in enacting Section 230 was to promote a vibrant marketplace to give users tools to provide a safe Internet experience for themselves and their families, without interference by state and federal regulation. By allowing plaintiffs to undermine the immunity granted by Section 230(c)(2)(B) and subjecting filtering-tool providers to prolonged and costly litigation, the Ninth Circuit's opinion accomplishes the opposite by interposing courts as regulators between Internet users and their choice of filtering tools.

Worse still, there is no logical limit to the Ninth Circuit's reasoning. Its ruling invites judges to chip away at all of Section 230(c)'s immunities, including the oft-invoked immunity of 230(c)(1) that protects websites from liability for third-party content. And because the Ninth Circuit's opinion is rooted in policy considerations unmoored from specific statutory text, it invites courts to impose additional policy-driven exceptions beyond the competition context.

A. The Decision Below Threatens The User Choice And Internet Security Goals That Motivated Section 230(c)(2)(B).

1. Congress's goal in enacting Section 230, and especially 230(c)(2)(B), was to put Internet users in

the driver's seat of their own online experience by allowing them to choose the filtering tools that best fit their needs without government interference. Congress recognized that services such as Malwarebytes's "offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops," and that the "Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation." 47 U.S.C. § 230(a)(2), (4). Congress thus declared that "the policy of the United States" is "to preserve the vibrant and competitive free market that presently exists for the Internet * * *, unfettered by Federal or State regulation"; "to encourage the development of technologies which maximize user control over what information is received"; and "to remove disincentives for the development and utilization of blocking and filtering technologies." *Id.* § 230(b)(2)-(4). As one of the bill's co-sponsors, Representative Chris Cox, explained, "every one of us will be able to tailor what we see to our own tastes" based on Section 230's promotion of a vibrant free market in filtering technology. 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox). In fact, Section 230 was introduced as a user-driven alternative to a bill that sought to combat offensive content through top-down government regulation. *See* Pet. App. 9a-11a.[6]

---

[6] Both provisions were enacted, but Section 230's government-regulation-based rival was largely invalidated by this Court for

As Judge Wilkinson put it in the first major circuit court decision on Section 230—since widely adopted by other courts—Congress created a "broad immunity" "to encourage service providers to self-regulate the dissemination of offensive material." *Zeran*, 129 F.3d at 331; *accord Jane Doe No. 1*, 817 F.3d at 29 ("Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections ***. Showing that a website operates through a meretricious business model is not enough to strip away those protections."). Part of Congress's motivation was to overrule a New York state court opinion, under which "computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher." *Zeran*, 129 F.3d at 331 (discussing *Stratton Oakmont*, 1995 WL 323710); *see also* Pet. App. 9a-10a; H.R. Conf. Rep. No. 104-458, at 194 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 10, 208. The statutory findings, policy statements, and legislative history thus all indicate a desire to let the market, and not courts, decide how content should be filtered.

But the Ninth Circuit's decision upsets the immunity that Congress created to achieve that goal. In place of the "broad immunity" prescribed by Congress, the Ninth Circuit has authorized courts to abrogate immunity for filtering decisions that, in the

---

violating the First Amendment. *See Reno* v. *ACLU*, 521 U.S. 844, 877-879 (1997).

court's opinion, Congress would not have wanted to protect. *See* Pet. App. 22a. Under that reasoning, any plaintiff can potentially convince a court to craft an exception for a particular set of facts or alleged motivation, thereby exposing the defendant to the whole panoply of state and federal statutory and common law causes of action that Congress sought to preempt. *See id.* at 13a-14a. So much for providers of filtering tools being "unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(2).

2. The possibility that a defendant will ultimately prove that it acted with motives a court would consider pure is little comfort. Congress created an *immunity* from suit precisely because, as Judge Wilkinson observed, it "recognized the threat that tort-based lawsuits pose" and so enacted Section 230 "to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum." *Zeran*, 129 F.3d at 330. As the same court later elaborated, "immunity is an *immunity from suit* rather than a mere defense to liability and it is effectively lost if a case is erroneously permitted to go to trial." *Nemet Chevrolet, Ltd.* v. *Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009) (internal quotation marks omitted). For that reason, "Section 230 immunity" should be "accorded effect at the first logical point in the litigation process." *Id.* In other contexts, this Court has recognized that immunities are not "merely * * * a defense to monetary liability," but rather "an immunity from suit" altogether, *Fed. Mar. Comm'n* v. *S.C. State Ports Auth.*, 535 U.S. 743, 766 (2002) (sovereign immunity), and "an entitlement not to

stand trial or face the other burdens of litigation," *Mitchell* v. *Forsyth*, 472 U.S. 511, 526 (1985) (qualified immunity).

If not afforded immunity from suit altogether, Internet services will "face death by ten thousand duck-bites." *Fair Hous. Council of San Fernando Valley* v. *Roommates.com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc). That is why "section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles." *Id.* at 1175.

The danger of abusive litigation in this area is no idle threat. That is because litigious malware purveyors can easily use the exception recognized by the Ninth Circuit to plead around Section 230(c)(2)(B) at the motion-to-dismiss stage. The decision below exacerbates that problem by setting a low bar for what a putative competitor must allege. *See* Pet. App. 23a (accepting Enigma's claims of "anticompetitive" behavior without enumerating specific facts).

It is not difficult for a purveyor of malware to brand themselves as an anti-malware provider by combining purported security features with objectionable material. For example, in an earlier Ninth Circuit case, the plaintiff combined a supposed "[s]pam [b]locker" with noxious adware that bombarded users with pop-up ads. *Zango*, 568 F.3d at 1170. After the decision below, any purveyor of malware and adware now has a playbook to overcome Section 230(c)(2)(B) simply by adding a purported security feature to their obnoxious software.

Even if the text of Section 230(c)(2)(B) gave courts license to second-guess the motivations for internet-

security firms' classification decisions, judges would be poorly positioned to do so. There are numerous valid reasons Internet-security firms may flag putatively competitive software as a threat. Even well-known brands have had security vulnerabilities or unexpectedly caused computers to slow down,[7] which could justify a potentially-unwanted-program label. More pernicious is fake antivirus software, a common problem that has been a target of government enforcement. Examples include a $163 million judgment the FTC obtained against an outfit that sold "scareware" to "trick consumers into thinking their computers were infected with malicious software, and then sold them software to 'fix' their non-existent problem"[8]; as well as a $35 million settlement with the well-known retailer Office Depot for marketing similar "scamware" that "tricked customers into buying millions of dollars' worth of computer repair and technical services by deceptively claiming their software had found malware symptoms on the customers' computers."[9] These firms could write a

---

[7] *See, e.g.*, Eric Griffith, *How to Rid a New PC of Crapware*, PCMag (Apr. 1, 2020), https://bit.ly/3ch9BMM (explaining that a well-known antivirus program is "likely to slow [a user's] PC").

[8] Press Release, FTC, *FTC Case Results in $163 Million Judgment Against "Scareware" Marketer* (Oct. 2, 2012), https://bit.ly/3bjkJIx.

[9] Press Release, FTC, *Office Depot and Tech Support Firm Will Pay $35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services* (Mar. 27, 2019), https://bit.ly/3afWpWH.

self-serving complaint like Enigma's to circumvent Section 230(c)(2)(B)'s immunity for cybersecurity firms that seek to protect consumers from these threats.

3. Congress instead intended consumers and their cybersecurity providers to evaluate Internet threats for themselves. By inviting courts to interpose themselves between consumers and cybersecurity services, the Ninth Circuit's decision threatens consumer choice and Internet security.

Purported "competitors" may in fact be legitimate threats to Internet users. *See supra* p. 26 & n.8. Moreover, with millions of potential threats on the Internet, it is impossible for filtering-software companies to individually analyze every potential danger to users. As the Electronic Frontier Foundation (EFF) and CAUCE North America, Inc. explained below, filtering software requires the use of automated algorithms to predict threats, which may sometimes flag potentially competitive software. EFF et al. C.A. *Amicus* Br. 9-10; *see also* ESET, LLC C.A. *Amicus* Br. 7-8 (explaining that Malwarebytes's competitor ESET "encounter[s] more than 300,000 new unique and suspicious objects every day" and that "it is not possible to sort through threats and other objectionable programs one by one and give deference to those that might plausibly claim to be competitors").

The Ninth Circuit's decision puts cybersecurity firms in a predicament. They can try their best to protect consumers against all threats, knowing that they will subject themselves to expensive lawsuits when they designate an alleged competitor as a

threat—either forcing them out of business or raising prices for consumers. Or they can avoid liability by taking a more permissive stance, exposing customers to threats. In either case, consumers end up with an inferior Internet experience. And facing such a choice, new firms may be dissuaded from entering the cybersecurity market altogether—exactly the opposite of what Congress wanted.

There is no need for those dire results. Section 230 has worked just as Congress intended to promote competition in filtering technology. Enigma's own complaint identified over 40 competing cybersecurity companies. C.A. E.R. 39.[10] The Ninth Circuit's justification for its policy-driven exception to Section 230(c)(2)(B) was a fear that such firms would "act for their own, and not the public, benefit" by adopting "filtering practices aimed at suppressing competition, rather than protecting internet users." Pet. App. 20a. In the "vibrant and competitive free market that presently exists * * * unfettered by Federal or State regulation," 47 U.S.C. § 230(b)(2), however, such a strategy would surely backfire. The reputational damage from self-serving filtering decisions would outweigh the benefits of dissuading a few

[10] This shows how unfounded the Ninth Circuit's competition concerns are in this market. In the antitrust context, such a competitive market would lead to prompt dismissal of any claim that a company had monopoly power. *See, e.g.*, *Eastman Kodak Co.* v. *Image Tech. Servs., Inc.*, 504 U.S. 451, 481 (1992) (giving examples of "nearly 100%," "80% to 95%," "87%," and "over two-thirds" as examples of market shares that could support a monopolization claim).

customers from trying a competitor's product. And if a customer does find that her cybersecurity provider is not acting in her interest, she has dozens of alternatives to choose from.

B. The Decision Below Will Undermine Other Tools That Help Internet Users Curate Their Own Online Experience.

The fallout of the Ninth Circuit's ruling will not be limited to cybersecurity software. Numerous online services—including tools offered by many of the most commonly used Internet products—are protected by Section 230(c)(2)(B)'s immunity. The Ninth Circuit's decision, if allowed to stand, will invite lawsuits against these companies' filtering decisions with ginned-up allegations of anticompetitive motives.

For example, Facebook gives users tools to hide or block content posted by others on their personal Facebook page and has successfully invoked Section 230(c)(2)(B) to defend those tools.[11] YouTube offers users "Restricted Mode": "an optional setting that you can use on YouTube to help screen out potentially mature content that you may prefer not to see or don't want others using your device to see."[12] Likewise, Twitter offers users a "quality filter" that allows them to "filter[ ] lower-quality content from [their] notifications," and it gives users tools to limit

---

[11] *Fehrenbach* v. *Zeldin*, No. 17-CV-5282 (JFB) (ARL), 2018 WL 4242452, at *5 (E.D.N.Y. Aug. 6, 2018), *report and recommendation adopted*, 2018 WL 4242453 (E.D.N.Y. Sept. 5, 2018).

[12] YouTube Help, *Disable or enable Restricted Mode*, Google, https://bit.ly/2KftqaQ (last visited May 11, 2020).

who can send them direct messages and to screen messages with "potentially sensitive" content. [13] Popular message-board website Reddit's entire content-moderation program relies on "[v]olunteer community moderators" who use Reddit-provided tools "to remove any post that does not follow their community's rules, without any involvement or direction from Reddit, Inc." [14]

These are all examples of tools that make the Internet a safer and more pleasant place for consumers. They are just the types of "action taken to enable * * * the technical means to restrict access to material" that Section 230(c)(2)(B) was meant to immunize. 47 U.S.C. § 230(c)(2)(B).

Yet under the Ninth Circuit's decision, Section 230(c)(2)(B) would no longer provide the kind of absolute immunity Congress intended "to encourage the development of technologies which maximize user control." *Id.* § 230(b)(3). Rather, plaintiffs whose content is flagged by these tools may write themselves an exception to Section 230(c)(2)(B) by alleging that YouTube or Reddit or Twitter acted with anticompetitive animus towards their content. Indeed, that is exactly what the plaintiff alleged in

---

[13] *About the Notifications timeline*, Twitter, https://bit.ly/3eu7VRv (last visited May 11, 2020); *About Direct Messages*, Twitter, https://bit.ly/3bldCQ2 (last visited May 11, 2020).

[14] *Transparency Report 2019*, Reddit, https://bit.ly/2ysFhj9 (last visited May 11, 2020) (showing that most removals are by user-moderators using Reddit-provided tools).

Prager, *supra* pp. 19-20, the decision that expressly disagreed with the Ninth Circuit's holding here.

C. The Decision Below Endangers All Of Section 230's Important Immunities.

The logic of the Ninth Circuit's decision also applies naturally to the rest of Section 230(c)'s immunities and will give courts license to imply additional exceptions beyond one for anticompetitive animus. The opinion's reasoning thus invites replacing the "broad immunity" that "Congress enacted," *Zeran*, 129 F.3d at 331, with an unpredictable quasi-immunity riddled with holes derived from judicial policy preferences.

1. Most obviously, any exception read into Section 230(c)(2)(B) would almost certainly apply to Section 230(c)(2)(A). After all, the "material" to which subsection (c)(2)(B) applies merely incorporates subsection (c)(2)(A)'s list by reference. Moreover, because subsection (c)(2)(A) has the "good faith" condition that (c)(2)(B) lacks, *see supra* pp. 14-15, any exception read into (c)(2)(B) would apply even more readily to (c)(2)(A).

But subsection (c)(2)(A) is crucial to what Congress intended when it enacted subsection (c) as a "[p]rotection for 'Good Samaritan' blocking and screening of offensive material." 47 U.S.C. § 230(c). As Judge Easterbook has explained, Section 230(c)(2) accomplishes that goal by working as a "safety net"; a "web host that * * * filter[s] out offensive material is not liable to the censored customer," thereby "induc[ing] web hosts * * * to take more care to protect the privacy and sensibilities of third parties." *Doe* v. *GTE Corp.*, 347 F.3d 655, 659-660 (7th Cir.

2003). That goal is understandable: An Internet where services like Facebook, YouTube, and Twitter could not screen graphically violent and sexual content for fear of facing massive litigation costs would be a scary place.

Yet the Ninth Circuit's insertion of atextual exceptions into Section 230(c)(2) will *discourage* moderation and restore the legal regime Congress intended to overturn with Section 230, in which content moderation creates liability. *See supra* p. 23. "Content moderation at scale is impossible to do well" because of the sheer complexity: services like Facebook receive hundreds of millions of uploads every day, requiring imperfect mass-automated moderation supported by thousands of human judgment calls.[15] Predictably, most anyone whose content is restricted will be upset. Under the Ninth Circuit's reasoning, so long as that person can come up with plausible allegations that the web service restricted the content in order to favor some competing content, the defendant will be unable to successfully invoke Section 230(c)(2) immunity at the motion-to-dismiss stage. Knowing that Section 230(c)(2) will offer only modest protection against litigious content-providers, interactive computer services will have a tremendous

---

[15] Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation At Scale Is Impossible To Do Well*, TechDirt (Nov. 20, 2019), https://bit.ly/2z1XpRh; *see* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv. L. Rev. 1598, 1635-48 (2018) (describing Facebook's multi-tiered, highly-complex moderation system).

incentive to scale back content moderation—exactly the opposite of the outcome Congress intended.

For example, Facebook's Community Standards include the platform's restrictions on hate speech, violent and graphic content, nudity and sexual activity, and sexual solicitation—all under the heading of "*Objectionable* Content."[16] That is the exact term used in Section 230(c)(2)'s catch-all provision. If courts fashion carve-outs to Section 230(c)(2) immunity for restricting "objectionable" content, purveyors of the most unpleasant software and material could fashion an exception for themselves.

2. The decision below also risks infecting the neighboring immunity in Section 230(c)(1). Whereas subsection (c)(2) immunizes actions to restrict or take down content, subsection (c)(1) immunizes the decision to leave up third-party content. Because the Ninth Circuit's purposive reasoning was not tethered to any text in (c)(2) and implied an exception from the findings and policy statements that apply to all of Section 230, there is nothing stopping plaintiffs from asking courts to fashion the same exception for (c)(1).

Subsection (c)(1) has been credited by many as having "[c]reated the Internet" as we know it today. *See, e.g.*, Jeff Kosseff, The Twenty-Six Words That Created the Internet 4 (2019) (explaining that nine of the ten most popular websites in the United States

---

[16] *Community Standards: Part III. Objectionable Content*, Facebook, https://bit.ly/2KgiUAq (last visited May 11, 2020) (emphasis added).

principally publish third-party content and so rely on Section 230(c)(1)). The vibrant Internet we know will be imperiled when plaintiffs seek to circumvent Section 230(c)(1)'s protections using the approach adopted by the Ninth Circuit below.

3. The fallout from the decision below is also not limited to anticompetitive motivation. Following in its logical footsteps, plaintiffs will ask courts to imply other exceptions based on the broad language in the findings and policy statements of Section 230(a) and (b). Prominent U.S. Senators have already done so, suggesting that subsection (a)(3)'s finding that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse" should be read to imply an immunity exception if a defendant's content moderation is not viewpoint-neutral.[17]

If plaintiffs can persuade judges that an Internet service is not providing "educational and informational resources" or "unique opportunities for cultural development," 47 U.S.C. § 230(a)(1), (3), or is not "promot[ing] the continued development of the Internet," *id.* § 230(b)(1), will the defendant lose Section 230 immunity? Such potentially far-reaching

---

[17] *See* Press Release, Senator Ted Cruz, *Sen. Cruz: The Pattern of Political Censorship Seen Across Technology Companies is Highly Concerning* (Jan. 17, 2018), https://bit.ly/2zdfuMB (Sen. Cruz committee-hearing comment suggesting that "if you are not a neutral public forum," then "the entire predicate for liability immunity" under Section 230 is not satisfied); Senator Josh Hawley (@HawleyMO), Twitter (Nov. 27, 2018, 1:22 PM), https://bit.ly/2VB3CLQ (suggesting same).

arguments will be hard to distinguish from the Ninth Circuit's use of the policy statements to limit the scope of immunity in this case.

III. THIS CASE IS AN IDEAL VEHICLE TO RESOLVE THE QUESTION PRESENTED, AND OTHER OPPORTUNITIES MAY NOT SOON PRESENT THEMSELVES.

1. This case presents an important and purely legal question to the Court without any complicating factual or procedural issues. The Ninth Circuit's ruling that Enigma's complaint should survive dismissal hinges entirely on a straightforward question of statutory interpretation about the scope of Section 230(c)(2)(B)'s immunity. That is an important question that is cleanly presented for this Court to answer.

2. Moreover, this Court may not soon get a better chance to answer the question presented. As the framers of Section 230 recognized, the cost of litigation may itself be enough to force defendants to settle. *See supra* pp. 5-6, 24-29. When facing onerous discovery and legal fees, providers like Malwarebytes may well have to capitulate to plaintiffs' demands not to be marked as threats, making the Internet a more dangerous place for consumers and depriving courts of the ability to provide further guidance on Section 230's immunities. If the Ninth Circuit's atextual exceptions leak into the surrounding provisions of Section 230, *see supra* pp. 31-34, Internet platforms deciding whether to filter offensive content or whether to remove third-party content challenged by a litigious plaintiff will have

similar incentives to settle rather than bear the cost of litigation.

Those dangers are especially heightened because of the Ninth Circuit's outsized role in the technology and Internet sphere. The decision below severely limited the main precedent that scholars have credited with dissuading suits nationwide against companies providing filtering tools.[18] Because so many technology companies are based within the Ninth Circuit, plaintiffs will often have the ability and incentive to bring suit in that circuit, minimizing the chances that another court of appeals or state court will be presented with the same question.

In short, by the time this Court is presented with another opportunity to evaluate whether Section 230 allows judge-made, policy-based exceptions, there is a great danger that filtering-software providers and others who rely on Section 230 will already have modified their business practices in response to the decision below, making the Internet a less safe and vibrant place for consumers.

---

[18] *See* Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 Tulane J. Tech. & Intell. Prop. 1, 6-7 (2017).

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

TYLER GRIFFIN NEWBY
FENWICK & WEST LLP
555 California Street
12th Floor
San Francisco, CA 94104

NEAL KUMAR KATYAL
Counsel of Record
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth St., N.W.
Washington, D.C. 20004
(202) 637-5600
neal.katyal@hoganlovells.com

Counsel for Petitioner

MAY 2020