

No. 19-1284

IN THE
Supreme Court of the United States

MALWAREBYTES, INC.,
Petitioner,

v.

ENIGMA SOFTWARE GROUP USA, LLC,
Respondent.

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

**BRIEF OF TECHFREEDOM AS *AMICUS CURIAE*
IN SUPPORT OF PETITIONER**

IAN SIMMONS
(Counsel of Record)
ANNA PLETCHER
STEPHEN MCINTYRE
MELISSA CASSEL
LAURA KAUFMANN
O'MELVENY & MYERS LLP
1625 Eye Street, N.W.
Washington, D.C. 20006
(202) 383-5300
isimmons@omm.com

BERIN SZÓKA
JAMES DUNSTAN
TECHFREEDOM
110 Maryland Avenue
N.E., Suite #205
Washington, D.C. 20002
mail@techfreedom.org

Attorneys for Amicus Curiae

TABLE OF CONTENTS

	Page
INTEREST OF <i>AMICUS CURIAE</i>	1
INTRODUCTION AND SUMMARY OF ARGUMENT.....	2
ARGUMENT	5
I. THE DECISION BELOW CONFLICTS WITH THIS COURT’S RULES OF STATUTORY INTERPRETATION	5
A. The Ninth Circuit Improperly Elevated Policy Over the Plain Meaning of the Text.....	5
B. The Decision Below Renders Section 230(c)(2) Incoherent by Obliterating the Distinction Between Subsections (c)(2)(A) and (c)(2)(B).....	8
II. THE DECISION BELOW THREATENS TO UNLEASH A FLOOD OF NEW LITIGATION THAT WILL REDUCE COMPETITION, INNOVATION, AND DIVERSITY IN THE INTERNET ECOSYSTEM.....	12

TABLE OF CONTENTS

	Page
A. The Decision Below Extends to Nearly Every Internet Tool, Not Just Cybersecurity Software	13
B. The Ninth Circuit’s Erroneous Interpretation of Subsection 230(c)(2)(B) Will Allow Myriad Claims That Congress Intended to Immunize	15
C. The Increased Costs of Doing Business Will Lead to a Less Competitive, Innovative, and Diverse Internet Ecosystem	17
CONCLUSION.....	19

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Baker Botts LLP v. ASARCO LLC</i> , 576 U.S. 121 (2015).....	3, 6
<i>Barnhart v. Sigmon Coal Co.</i> , 534 U.S. 438 (2002).....	5
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	17
<i>Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.</i> , 511 U.S. 164 (1994).....	6
<i>Conn. Nat’l Bank v. Germain</i> , 503 U.S. 249 (1992).....	6
<i>Crawford Fitting Co. v. J.T. Gibbons, Inc.</i> , 482 U.S. 437 (1987)	17
<i>Dombrowski v. Pfister</i> , 380 U.S. 479 (1965).....	18
<i>e360Insight, LLC v. Comcast Corp.</i> , 546 F. Supp. 2d 605 (N.D. Ill. 2008).....	10
<i>Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.</i> , 946 F.3d 1040 (9th Cir. 2019).....	passim
<i>Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC</i> , 521 F.3d 1157 (9th Cir. 2008).....	4
<i>Hecht v. Pro-Football, Inc.</i> , 444 F.2d 931 (D.C. Cir. 1971).....	6

TABLE OF AUTHORITIES
(continued)

	Page(s)
<i>Law v. Siegel</i> , 571 U.S. 415 (2014).....	7
<i>Nemet Chevrolet, Ltd. v.</i> <i>Consumeraffairs.com, Inc.</i> , 591 F.3d 250 (4th Cir. 2009).....	17
<i>NRG Power Mktg. LLC v. Me. Pub. Util.</i> <i>Comm’n</i> , 558 U.S. 165 (2010)	4
<i>Race Tires Am., Inc. v.</i> <i>Hoosier Racing Tire Corp.</i> , 614 F.3d 57 (3d Cir. 2010)	18
<i>Romag Fasteners, Inc. v. Fossil, Inc.</i> , 140 S. Ct. 1492 (2020).....	5, 6, 7
<i>Rowe v. N.H. Motor Transp. Ass’n</i> , 552 U.S. 364 (2008).....	7
<i>Zango, Inc. v. Kaspersky Lab, Inc.</i> , 568 F.3d 1169 (9th Cir. 2009).....	8, 9
STATUTES	
7 U.S.C. § 291	7
7 U.S.C. § 292	7
15 U.S.C. § 1	7
15 U.S.C. § 26b	7
15 U.S.C. § 1013	7
47 U.S.C. § 230	2
47 U.S.C. § 230(b)(1)	18
47 U.S.C. § 230(b)(2)	18

TABLE OF AUTHORITIES
(continued)

	Page(s)
47 U.S.C. § 230(b)(3)	18
47 U.S.C. § 230(b)(4)	14
47 U.S.C. § 230(c)(2).....	3
47 U.S.C. § 230(c)(2)(A).....	5, 8
47 U.S.C. § 230(c)(2)(B).....	2, 5, 11
47 U.S.C. § 230(e).....	7
47 U.S.C. § 230(f)(2)	10
 OTHER AUTHORITIES	
141 Cong. Rec. H 8425, 8469	15
GIFCT, Joint Tech Innovation	9
Google, Your Content & Restricted Mode	10
Memorandum from Paul V. Niemeyer, Chair, Advisory Committee on Civil Rules, to Hon. Anthony J. Scirica, Chair, Committee on Rules of Practice and Procedure (May 11, 1999), 192 F.R.D. 354 (2000).....	17
Net Nanny, Block Apps.....	16
YouTube, YouTube Trusted Flagger Program.....	10

**BRIEF OF TECHFREEDOM
AS *AMICUS CURIAE* IN SUPPORT OF
PETITIONER**

TechFreedom respectfully submits this brief as *amicus curiae* in support of Malwarebytes, Inc.’s petition for a writ of certiorari.¹

INTEREST OF *AMICUS CURIAE*

TechFreedom is a nonprofit, nonpartisan think tank based in Washington, D.C. Its work on information technology policy is founded on the belief that technology enhances freedom and freedom enhances technology. Consistent with that principle, TechFreedom has long been involved in debates over Internet freedom, free speech, privacy, and data security. Since its founding in 2010, TechFreedom has published half a dozen white papers addressing Section 230 of the Communications Decency Act and regularly provided lawmakers with detailed legal analysis concerning Section 230’s immunity provisions. Congress has also invited TechFreedom to provide testimony based on its deep knowledge of Section 230.

TechFreedom believes the Ninth Circuit’s interpretation of Subsection 230(c)(2)(B) of the Communications Decency Act is unsupported by the text of the

¹ Counsel for *amicus curiae* state that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person or entity other than *amicus curiae* or its counsel has made a monetary contribution to the preparation or submission of this brief. All parties received notice of TechFreedom’s intent to file this brief at least ten days before the filing deadline. The parties have consented in writing to the filing of this brief.

statute and stifles competition, innovation, and consumer choice across the Internet ecosystem.

INTRODUCTION AND SUMMARY OF ARGUMENT

Section 230 of the Communications Decency Act makes websites and their users, rather than courts or governments, the regulators of their own Internet experiences. *See* 47 U.S.C. § 230. Critical to that infrastructure is Section 230(c), which immunizes providers and users of interactive computer services (“ICS”) from litigation for publishing, moderating, or removing objectionable content posted or created by third parties. The first provision, Section 230(c)(1), states that ICS providers and users will not be treated as the publishers or speakers of any information posted by another Internet provider or user. The second provision, Subsection 230(c)(2)(A), immunizes providers and users who in good faith filter or remove content that they consider objectionable. This case deals with the third provision, Subsection 230(c)(2)(B), which grants immunity to those who provide *others* with the “technical means” to filter or restrict access to content that they deem objectionable.

Subsection 230(c)(2)(B) contains a simple command: “No provider or user of an interactive computer service shall be held liable [for] any action taken to enable or make available . . . the technical means to restrict access to [objectionable] material.” *Id.* § 230(c)(2)(B). That’s it. But when the Ninth Circuit interpreted this statute, it saw something different. Speculating that a strict textual interpretation would lead to a result that “appear[ed] contrary to [the statute’s] history and purpose,” the court divined words

invisible to the human eye: an exception for conduct allegedly motivated by “anticompetitive animus.” *Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1050 (9th Cir. 2019). That exception is nowhere to be found in the statute that Congress enacted.

This Court should grant certiorari because the Ninth Circuit’s misinterpretation of Subsection 230(c)(2)(B)’s plain text ignores this Court’s canons of statutory interpretation and will have grave consequences for innovation, consumer choice, and diversity across the Internet ecosystem.

1. The Ninth Circuit’s decision cannot be reconciled with this Court’s rules of statutory interpretation because it is based on judicial policy judgments rather than the text of the statute. *Baker Botts LLP v. ASARCO LLC*, 576 U.S. 121, 135 (2015) (explaining that courts cannot rewrite statutes based on their own policy preferences). Making matters worse, the decision below renders the statute incoherent. While Congress chose to include a good-faith requirement in Subsection 230(c)(2)(A), which bestows immunity on those who decide to restrict access to online content, it deliberately omitted that same requirement from Subsection 230(c)(2)(B) for those who provide the “technical means” for *others* to restrict access to content. *See* 47 U.S.C. § 230(c)(2). The Ninth Circuit’s decision obliterates this distinction.

2. The decision below will have far-reaching adverse consequences for the Internet, which touches virtually every aspect of daily life. By reading in an unstated exception to the immunities provided in Subsection 230(c)(2)(B), the Ninth Circuit’s ruling

promises a flood of new litigation against a range of people and innovators far broader than just developers of anti-malware software. Exacerbating this problem, the Ninth Circuit’s decision opens the door to a panoply of state and federal causes of action that are predicated on allegations of bad faith or unfair competition. Not only does litigation impose a substantial new cost on existing competitors, the specter of protracted legal battles will deter new players from entering the market in the first place—leading to a less competitive, innovative, and diverse Internet for everyone. In effect, the decision will subject cybersecurity and filtering software companies to “death by ten thousand duck-bites.” *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1174-75 (9th Cir. 2008) (en banc) (explaining that “[S]ection 230 must be interpreted to protect websites not merely from ultimately liability, but from having to fight costly and protracted legal battles”). The Ninth Circuit’s creation of a new exception for anti-competitive animus is, ironically, *anticompetitive*.

If this Court does not act, these consequences will soon reverberate nationwide. Because the Ninth Circuit encompasses the nation’s epicenter of technological innovation, its decision has the potential to impact every American’s Internet experience. It portends a less competitive and more litigious Internet, creating uncertainty where there should be none, all to the detriment of Internet users. This Court has intervened to correct flawed decisions that promise widespread consequences in the past; it need not, and should not, wait for further division among courts. *See, e.g., NRG Power Mktg. LLC v. Me. Pub. Util. Comm’n*, 558 U.S. 165, 171 (2010). This Court should grant the petition

for certiorari to correct the Ninth Circuit’s flawed interpretation of Subsection 230(c)(2)(B) now.

ARGUMENT

I. THE DECISION BELOW CONFLICTS WITH THIS COURT’S RULES OF STATUTORY INTERPRETATION.

A. The Ninth Circuit Improperly Elevated Policy Over the Plain Meaning of the Text.

Section 230(c)(2) houses two separate immunity provisions. Subsection 230(c)(2)(A) provides immunity for those who block or filter content that they consider to be offensive. 47 U.S.C. § 230(c)(2)(A). For this immunity to apply, the person or entity must act “in good faith.” *Id.* Subsection 230(c)(2)(B) extends immunity to those that provide *others* with the “technical means” to filter or restrict access to content. *Id.* § 230(c)(2)(B). In this latter immunity provision, Congress omitted any good-faith requirement. *See id.* The Ninth Circuit majority concluded that this omission was ill-advised. And so it did some editing.

In ruling that Subsection 230(c)(2)(B) contains an exception for conduct allegedly motivated by “anti-competitive animus,” the Ninth Circuit flouted this Court’s instruction that “courts must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 461-62 (2002) (quotation omitted). This Court does not “read into statutes words that aren’t there.” *Romag Fasteners, Inc. v. Fossil, Inc.*, 140 S. Ct. 1492, 1495 (2020). That remains true even if a court believes Congress’s chosen words “lead to a harsh outcome” or seemingly “undercut a basic

objective of the statute.” *Baker Botts*, 576 U.S. at 135 (quotations omitted). A court’s “job is to follow the text.” *Id.*; see *Romag Fasteners*, 140 S. Ct. at 1497 (“This Court’s limited role is to read and apply the law [that] policymakers have ordained[.]”); *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 188 (1994) (“Policy considerations cannot override our interpretation of the text and structure of the Act[.]”). This is no technicality; the Constitution does not bestow upon courts “the authority to rewrite [] statute[s].” *Baker Botts*, 576 U.S. at 135. That prerogative belongs to Congress.

The Ninth Circuit defied this “cardinal canon” of statutory interpretation. See *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992). By fashioning an “anticompetitive animus” exception to Subsection 230(c)(2)(B)’s near-categorical immunity, the Ninth Circuit elevated its own policy considerations over Congress’s chosen words. It did exactly what this Court has admonished: it rewrote the statute to add a new exception from immunity based on its assumption that adhering to the statutory text would “lead to a harsh outcome” and “undercut” desirable policy goals. See *Baker Botts*, 576 U.S. at 135 (quotations omitted). It is not the role of the judiciary to decide what is “desirable as a matter of policy.” *Id.*

The structure of Section 230(c) is no accident. Congress knows how to craft immunities, including for anticompetitive conduct. See *Hecht v. Pro-Football, Inc.*, 444 F.2d 931, 943-44 (D.C. Cir. 1971) (“Congress knows how to spell out an exemption from the anti-trust law when it wants to do so.”). Time and again, Congress has made the policy judgment that particu-

lar classes of economic actors or conduct warrant immunity from suit, even if they might otherwise be deemed anticompetitive in purpose or effect. *See, e.g.*, McCarran-Ferguson Act, 15 U.S.C. § 1013 (insurance exemption); Curt Flood Act, 15 U.S.C. § 26b (baseball exemption); Capper-Volstead Act, 7 U.S.C. §§ 291-92 (farm cooperative exemption). Congress chose not to write an antitrust exception into Section 230.

Congress *did* include some carve-outs from immunity, including for federal criminal offenses and for laws dealing with intellectual property, communications privacy, and sex trafficking. *See* § 47 U.S.C. § 230(e).² That specific, codified list underscores “that courts are not authorized to create additional exemptions” to Subsection 230(c)(2)(B). *See Law v. Siegel*, 571 U.S. 415, 424 (2014); *see also Rowe v. N.H. Motor Transp. Ass’n*, 552 U.S. 364, 374 (2008) (refusing to infer a “public health exception” to the Federal Aviation Administration Authorization Act of 1994 because the Act “explicitly lists a set of exceptions (governing motor vehicle safety, certain local route controls, and the like), but the list says nothing about public health”). The Ninth Circuit’s “limited role” was to apply the law as Congress wrote it, not to craft new exceptions that Congress chose to leave out. *See Romag Fasteners*, 140 S. Ct. at 1497.

² Because Section 230(c) does not immunize federal criminal offenses, the statute would not preclude the government from prosecuting criminal Sherman Act violations. *See* 15 U.S.C. § 1 (providing for criminal penalties).

B. The Decision Below Renders Section 230(c)(2) Incoherent by Obliterating the Distinction Between Subsections (c)(2)(A) and (c)(2)(B).

Compounding its error, the Ninth Circuit’s decision also renders the statute incoherent. Unlike Subsection 230(c)(2)(A), which requires those who actually restrict content—for example, a website that removes an offensive post—to act in “good faith,” Subsection 230(c)(2)(B) applies only to those who provide others with the “technical means to restrict access to material described in [Subsection 230(c)(2)(A)].”³ While Subsection 230(c)(2)(B) incorporates the *material* described in 230(c)(2)(A),⁴ it does not adopt its good-faith requirement. That is because the good-faith requirement *precedes* the clause describing the material. *See* 47 U.S.C. § 230(c)(2)(A) (immunizing “any action voluntarily taken in good faith to restrict access to or availability of material . . .”). By design, the good-faith requirement does not apply to Subsection 230(c)(2)(B).

Section 230(c)(2)’s structure is perfectly logical. It would not make any sense to hold providers of filtering tools liable based on *users’* decisions to “purchase, install, and utilize” those tools to tailor their Internet

³ Courts uniformly recognize Subsection 230(c)(2)(B)’s reference to Section 230(c)(1) as a “typographical error.” *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 n.5 (9th Cir. 2009).

⁴ Subsection 230(c)(2)(A) immunizes providers and users from liability for restricting access to “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.” 47 U.S.C. § 230(c)(2)(A).

experiences. *Zango*, 568 F.3d at 1176. Nor would it make sense to hold developers liable when they provide those tools to other ICS providers.⁵ Yet the Ninth Circuit’s ruling authorizes both.

And all for no good reason. The majority’s creation of an “anticompetitive animus” exception to Subsection 230(c)(2)(B) was purportedly driven by a “warning” Judge Fisher voiced a decade ago in a concurring opinion in another case: that if the statute were construed according to its “literal terms,” Subsection 230(c)(2)(B) could immunize “covert, anti-competitive blocking” of desirable content “without the user’s knowledge.” *Zango*, 568 F.3d at 1178-79 (Fisher, J., concurring) (emphasis omitted); see *Enigma*, 946 F.3d at 1045. But this concern evinces a misunderstanding of the statute. In Judge Fisher’s hypothetical, a software developer’s decision to covertly block a competitor’s content would not implicate Subsection 230(c)(2)(B) in the first place; when an ICS provider acts *independently* of the end user (or parent or other

⁵ For example, the Global Internet Forum to Counter Terrorism (GIFCT) is an independent nonprofit that maintains “a shared industry database of ‘hashes’—unique digital ‘fingerprints’—for violent terrorist imagery or terrorist recruitment videos that [it has] removed from [its] services.” GIFCT, Joint Tech Innovation, <https://www.gifct.org/joint-tech-innovation> (last visited June 9, 2020). GIFCT’s thirteen member companies, which include Google, Facebook, Twitter, and Instagram, rely on the database to “identify and remove matching content—videos and images—that violate [their] respective policies or, in some cases, block terrorist content before it is even posted.” *Id.* The plain text of Subsection 230(c)(2)(B) protects GIFCT’s development and provision of the tool to its members without requiring a showing of good faith.

intermediary⁶) to restrict access to material on its own service, its conduct falls squarely under Subsection 230(c)(2)(A). And under that provision, the provider has to act with good faith.

Consider, for example, email. When an email service automatically designates particular messages as “spam” and relegates them to a spam folder, the service “restricts access” to information that is contained within its own service—and does so independently of any action by the user. This filtering is governed by Subsection 230(c)(2)(A), meaning that the good-faith requirement applies. *See e.g., e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008). That remains true even if users can later comb their mailboxes and un-flag specific emails; the locus of control resides with the ICS provider itself.⁷

⁶ Schools and libraries, for example, use a variety of filtering tools to limit access by their students, visitors, and patrons to content the schools or libraries deem objectionable. One of those tools is YouTube’s Restricted Mode, which, if activated by a parent or institutional administrator, automatically blocks videos flagged as portraying objectionable content (*e.g.*, drugs and alcohol, sexual situations, violence, mature language. *See* Google, Your Content & Restricted Mode, <https://tinyurl.com/yaow8hw5> (last visited June 11, 2020). Congress plainly intended for Subsection 230(c)(2)(B) to cover these technologies, as it specifically included “libraries or educational institutions” in the definition of “interactive computer service.” 47 U.S.C. § 230(f)(2).

⁷ YouTube’s “Trusted Flagger” program, which “provide[s] robust tools for individuals, government agencies, and non-governmental organizations (NGOs) that are particularly effective at notifying YouTube of content that violates [its] Community Guidelines,” provides another example of when Subsection 230(c)(2)(B) does, and does not, apply. *See* YouTube, YouTube Trusted Flagger Program, <https://support.google.com/youtube/>

Things are different when an ICS provider either facilitates content restriction with respect to a third-party service or empowers users of its own service to take such action. In these scenarios, the provider merely acts to “enable or make available” the technical means to restrict access—bringing it within the ambit of Subsection 230(c)(2)(B). 47 U.S.C. § 230(c)(2)(B). For example, if an email service provider does not catch enough spam, the user might add another line of defense through a third-party filter. Unlike the original email service provider, that third-party filter provides the user with the tools to *proactively* quarantine more spam. And so, a shift in decision-making occurs: the user wields control. In this circumstance, the provider of the third-party filter enjoys immunity under Subsection 230(c)(2)(B), regardless of good faith.

The Ninth Circuit failed to appreciate this distinction, exacerbating its error. Unlike the email service that quarantines spam independently of its users’ actions, Malwarebytes makes the user the decision-maker. The user downloads Malwarebytes for the very purpose of flagging potentially unwanted programs, and once Malwarebytes flags those programs, the user has full discretion over whether to quarantine and remove them. Indeed, Malwarebytes provides its users with context to help them make in-

[answer/7554338?hl=en](https://www.fcc.gov/answer/7554338?hl=en) (last visited June 11, 2020). When YouTube uses these tools to make decisions about its *own* platform, it is not protected by Subsection 230(c)(2)(B) because it restricts access to information contained within its own service. By contrast, YouTube’s provisioning of these tools to Trusted Flagger *would* be covered by Subsection 230(c)(2)(B).

formed filtering decisions; this allows even non-technical users to retain control over their filtering decisions. And, critically, that locus of control places Malwarebytes squarely within the ambit of Subsection 230(c)(2)(B), under which there is no good-faith requirement.

That means that the Ninth Circuit majority not only disregarded this Court’s well-established statutory interpretation rules, but also collapsed the entire infrastructure rendering Section 230(c)(2) coherent: different requirements for different decision-makers.

II. THE DECISION BELOW THREATENS TO UNLEASH A FLOOD OF NEW LITIGATION THAT WILL REDUCE COMPETITION, INNOVATION, AND DIVERSITY IN THE INTERNET ECOSYSTEM.

The most likely effect of the Ninth Circuit’s erroneous ruling is an influx of new litigation. That is true for at least two reasons. First, the immunity that Congress created through Subsection 230(c)(2)(B) protects more than just cybersecurity software—it extends to content filtering and moderation tools used across the Internet. Second, the decision below invites other claims predicated on alleged bad-faith conduct from plaintiffs whose content was blocked or filtered. Taken together, these incentives to litigate and loss of immunity threaten to chill innovation, deter competition, and reduce consumer choice.⁸

⁸ That consequence is particularly acute given the low bar the Ninth Circuit majority set: it ruled that alleging “anticompetitive animus” is all it takes to defeat Subsection 230(c)(2)(B) immunity at the pleading stage and unlock the door to years of bur-

A. The Decision Below Extends to Nearly Every Internet Tool, Not Just Cybersecurity Software.

Cybersecurity is not the only industry that provides consumers with the technology to filter or block content. When the Ninth Circuit fashioned its judicially-created exception to Subsection 230(c)(2)(B) immunity, it did so within the cybersecurity context. But the countless products that give consumers the “technical means” to filter content—from security threats to unwanted advertisements, hate speech, and pornography—make the consequences of the Ninth Circuit’s ruling even more pronounced.

For example, parents can use online tools like Net Nanny to make the Internet safer for their children. *See* Net Nanny, <https://www.netnanny.com> (last visited June 9, 2020). These products allow parents to shield their children from content they deem inappropriate, like hateful speech and indecency. Like anti-malware software, these tools put the filtering decisions in the hands of the consumer: parents decide which (if any) tool to use, based on their family’s needs and preferences, and then configure those tools to block, filter, or otherwise moderate content they deem objectionable. Put simply, parental control products enable parents to decide how and when to cover their children’s eyes.⁹

densome discovery and litigation. *Enigma*, 946 F.3d at 1052. Notably, *Enigma* did not even raise any antitrust claims, and it is unlikely that it *could* have plausibly alleged any anticompetitive harm, since Malwarebytes does not possess market power. *See* Pet. 28-29 & n.10.

⁹ Section 230 itself states that one of its purposes is “to remove disincentives for the development and utilization of blocking and

Under the Ninth Circuit’s ruling, an aggrieved advertiser could easily defeat the parental control service’s immunity under Subsection 230(c)(2)(B). Consider this: parents might use Net Nanny or similar software to block all advertisers or phishing schemes from reaching their children. It’s not a stretch to think that some of those advertisements might be from competing parental control tools—indeed, an advertiser using data analytics to target potential consumers would probably advertise to the *exact* same people who are likely to already use parental controls. If the developer of another parental control tool then sues the developer of the first, perhaps alleging a tortious interference with business claim, it could overcome Subsection 230(c)(2)(B) immunity with fewer words than are in this sentence: “Defendant acted with anticompetitive animus.”

Or take, as another example, Social Fixer, a popular online application that allows consumers to tailor the content they receive on Facebook. *See* Social Fixer, <https://www.socialfixer.com> (last visited June 9, 2020). With a few clicks, consumers can hide posts involving specified keywords or authors, filter out political content, or block targeted advertisements. Like parental tools, Social Fixer puts the consumer in control; in the language of Subsection 230(c)(2)(B), it provides the “technical means” by which the consumer chooses what fills her computer screen.

A similar situation to the parental control context could play out here. Using Social Fixer, a consumer

filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material[.]” 47 U.S.C. § 230(b)(4).

could block all targeted advertisements. Some of those advertisements might be from *other* filtering programs, like AdBlock or FB Purity, that compete with Social Fixer. This means that when Social Fixer’s competitor sues for tortious interference or unfair competition, it has a built-in argument to overcome the immunity Congress enacted.

These examples illustrate just how far the Ninth Circuit’s ruling extends. The ubiquitous threat of litigation will disrupt the Internet ecosystem—the very ecosystem Congress deliberately kept out the courtroom. *See* 141 Cong. Rec. H 8425, 8469 (noting that, before the statute, the “existing legal system provide[d] a massive disincentive for the people who might best help us control the Internet to do so”).

B. The Ninth Circuit’s Erroneous Interpretation of Subsection 230(c)(2)(B) Will Allow Myriad Claims That Congress Intended to Immunize.

It is not hard to imagine how the Ninth Circuit’s decision may lead to broader immunity carve-outs, beyond allegations of “anticompetitive animus.” By reading an implicit good-faith limitation into unqualified language, the Ninth Circuit invites creative litigants to assert an array of federal and state-law claims predicated on bad-faith conduct. The Internet will become a hotbed of litigation—exactly the opposite of what Congress intended.

In the decision below, the Ninth Circuit created the “anticompetitive animus” exception to allow a federal Lanham Act claim and state-law claims based on deceptive business practices and tortious interference

with business and contractual relations to proceed. *Enigma*, 946 F.3d at 1048. The Ninth Circuit decision will expose cybersecurity and filtering software companies to other claims that require a showing of bad faith or animus, including the Lanham Act, state and common-law torts, unfair competition, commercial disparagement, and false advertising.

The range of factual scenarios that may now expose one to litigation is not limited to disputes involving “anticompetitive animus.” The Ninth Circuit’s erroneous reading of a good-faith requirement into Subsection 230(c)(2)(B) invites courts to read *other* non-existent exceptions into the statute. For example, a consumer may use a program like Net Nanny to prevent his or her children from accessing content on certain smartphone applications that he or she deems inappropriate. Notably, the Net Nanny filtering application for iOS devices “includes an estimated 125 of the most common and concerning apps for parents.” Net Nanny, Block Apps, <https://www.netnanny.com/features/block-apps> (last visited June 9, 2020). Companies whose advertisements or other content were blocked, but whose products do not compete with Net Nanny, could potentially bring an action for false advertising or commercial disparagement because the application flagged them to the user as “concerning” or “inappropriate,” and a court could apply the Ninth Circuit’s reasoning to imply an exception for defamatory intent.

The majority’s ruling all but entirely dislodges the broad immunity that Congress prescribed. It not only conjures up an unstated and nontextual exception, but does so in a way that invites litigation across a

litany of industries and claims. And it beckons plaintiffs to glide past the motion-to-dismiss stage with allegations of “animus” or other “bad faith,” eviscerating the very notion of immunity. *See Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009) (explaining that “immunity is an *immunity from suit* rather than a mere defense to liability and is effectively lost if a case is erroneously permitted to go to trial”).

C. The Increased Costs of Doing Business Will Lead to a Less Competitive, Innovative, and Diverse Internet Ecosystem.

Regardless of ultimate liability, litigation is burdensome—in time, reputational costs, stress, and money. As this Court has observed, the “costs of litigation, as we all know, have become staggering. A plaintiff may put a defendant or a defendant may put a plaintiff to a tremendous amount of expense . . . in defending or prosecuting a case.” *Crawford Fitting Co. v. J.T. Gibbons, Inc.*, 482 U.S. 437, 450 (1987). The bulk of that expense—sometimes up to 90 percent—arises out of discovery. *See* Memorandum from Paul V. Niemeyer, Chair, Advisory Committee on Civil Rules, to Hon. Anthony J. Scirica, Chair, Committee on Rules of Practice and Procedure (May 11, 1999), 192 F.R.D. 354, 357 (2000) (reporting that discovery accounts for as much as 90 percent of litigation costs).

That is particularly true in the antitrust context. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558-59 (2007) (noting that the mere “threat of discovery expense will push cost-conscious defendants to settle

even anemic cases before reaching those proceedings”). And it holds true even if the defendant prevails at summary judgment or trial. See *Dombrowski v. Pfister*, 380 U.S. 479, 487 (1965) (“The chilling effect . . . [of litigation is] unaffected by the prospects of its success or failure.”).

Perversely, the Ninth Circuit’s concern for anti-competitive animus may actually *reduce* competition. The substantial costs of litigation could put smaller companies out of business and deter others from entering the market altogether. See, e.g., *Race Tires Am., Inc. v. Hoosier Racing Tire Corp.*, 614 F.3d 57, 73 (3d Cir. 2010) (“[L]engthy and drawn-out litigation . . . may have a chilling effect on competitive market forces.”); While larger companies may weather the litigation storm, smaller players and new entrants might not. The costs may be too high for new mavericks to justify entering or staying in a market.

That means there will be less innovation and less diversity across the Internet, leaving users with fewer (and perhaps worse) options for fashioning the Internet experiences that they want.¹⁰ What’s more, the threat of costly litigation will also incentivize developers to err on the side of *not* filtering or flagging borderline content, meaning that Internet users will

¹⁰ That result is the opposite of the first three stated policy goals of Section 230: “to promote the continued development of the Internet and other interactive computer services and other interactive media”; “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”; and “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[.]” 47 U.S.C. §§ 230(b)(1)-(3).

be *less* protected. This cuts *against* Subsection 230(c)(2)(B)’s safe harbor for technological tools that empower families and consumers to curate their Internet experiences.

And as smaller industry players are pushed out, their products—which might otherwise have benefited users and injected markets with needed innovation and competition—will be absent. Although the Ninth Circuit opined that interpreting Subsection 230(c)(2)(B) as Congress wrote it “would lessen user control over what information they receive,” *Enigma*, 946 F. 3d at 1051, it is the Ninth Circuit’s rewrite of that provision that presages that outcome.

The impact of the Ninth Circuit’s error is not cabined to its flouting of the statutory text. It will also stifle competition, innovation, and consumer choice across the Internet ecosystem. This Court should grant certiorari to clarify that that provision does not contain an exception for “anticompetitive animus.”

CONCLUSION

For the foregoing reasons and those in the petition, the petition for a writ of certiorari should be granted, or alternatively, the decision below should be summarily reversed.

Respectfully submitted,

IAN SIMMONS
(*Counsel of Record*)

ANNA PLETCHER

STEPHEN MCINTYRE

MELISSA CASSEL

LAURA KAUFMANN

O'MELVENY & MYERS LLP

1625 Eye Street, N.W.

Washington, D.C. 20006

(202) 383-5300

isimmons@omm.com

BERIN SZÓKA

JAMES DUNSTAN

TECHFREEDOM

110 Maryland Ave

N.E., Suite #205

Washington, D.C. 20002

mail@techfreedom.org

Counsel for Amicus Curiae

June 12, 2020