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 ESET, LLC AS AMICUS CURIAE IN SUPPORT OF PETITIONER MALWAREBYTES

ANNA-ROSE MATHIESON
Counsel of Record
Susan Yorke
CALIFORNIA APPELLATE LAW GROUP LLP
96 Jessie Street
San Francisco, CA 94105
(415) 649-6700
annarose@calapplaw.com

Attorneys for Amicus Curiae ESET, LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

TABLE OF AUTHORITIES (continued)

Page

TABLE OF AUTHORITIES (continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

BRIEF OF ESET, LLC AS AMICUS CURIAE IN SUPPORT OF PETITIONER

The undersigned respectfully submit this amicus curiae brief in support of Petitioner Malwarebytes.[1]

INTERESTS OF AMICUS CURIAE

Amicus curiae ESET, LLC is an award-winning cyber security company driven by innovative research and development. It is part of a worldwide group of companies that protects over 110 million users and operates in over 200 countries. ESET's mission is to protect its users from cyber threats, to provide users with control over their internet experience, and to build a more secure digital world.

ESET submits this amicus brief in the spirit of that mission. ESET competes vigorously with petitioner Malwarebytes in the market for cyber security products, yet this case involves a question of such exceptional importance that ESET decided to file an amicus brief in support of one of its direct competitors. Unless this Court grants certiorari, it will be harder for ESET and other legitimate cyber security companies to provide their users with the means to avoid objectionable materials online, and the internet will

---

[1] Amicus notified all parties of its intent to file this brief more than ten days before the due date, and all parties consented to the filing of this brief. No counsel for a party authored the brief in whole or in part, no party or party's counsel made a monetary contribution intended to fund the preparation or submission of this brief, and no person or entity, other than the amicus curiae or its counsel, made a monetary contribution to the preparation or submission of this brief.

become a more dangerous and confusing place for consumers.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

The Ninth Circuit's opinion undermines internet security and harms consumer choice in at least two critical ways.

First, the opinion impedes the development of effective cyber security software. Congress granted broad immunity to companies that provide users the means to filter out objectionable online content, but the Ninth Circuit's decision undercuts that statutory immunity whenever a plaintiff alleges anticompetitive animus. Yet a purveyor of objectionable material can easily position itself as a competitor and make a facially plausible claim of such animus. Because of the expense involved in defending litigation past the pleading stage, the decision discourages software companies from developing effective filtering and blocking tools. This undermines Congress's goals in enacting the Communications Decency Act, 47 U.S.C. § 230 (1996) (CDA), and harms the procompetitive interests the Ninth Circuit's opinion purports to protect.

Second, the decision substitutes judicial intervention for the user choice that has created a thriving marketplace of cyber security protections. Such choice now exists at two levels: when the user decides what security software to deploy, and when the user chooses to filter out an objectionable program with the aid of that software. The Ninth Circuit's opinion would substitute litigation in which the user has no role for both choices.

The Ninth Circuit's interpretation of the CDA defies the statute's plain text and undermines its policy goals. This Court's review is warranted for all the reasons set out in the petition.

ESET takes the unusual step of submitting an amicus brief in support of one of its direct competitors to stress the importance of this issue. Americans are becoming increasingly reliant on the internet and interactive media for political, educational, cultural, and entertainment services.[2] 47 U.S.C. § 230(a)(5). Yet security threats are flourishing, with hundreds of thousands of new forms of objectionable content every day. Congress determined that consumer choice and robust competition are the best way to safeguard consumers, but the Ninth Circuit's decision frustrates both choice and competition. Amicus ESET urges this Court to grant review.

ARGUMENT

Congress passed the CDA in part "to encourage the development of technologies which maximize user

---

[2] The recent pandemic has brought this reliance into sharp relief. *See, e.g.*, Ella Koeze & Nathaniel Popper, *The Virus Changed the Way We Internet*, N.Y. Times (Apr. 7, 2020), https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html; Jim Boehm et al., *Cybersecurity Tactics for the Coronavirus Pandemic*, McKinsey & Company (Mar. 27, 2020), https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-tactics-for-the-coronavirus-pandemic; World Economic Forum, *Cybersecurity Leadership Principles: Lessons Learnt During the COVID-19 Pandemic to Prepare for the New Normal* (May 26, 2020), *available at* https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal.

control over what information is received by individuals, families, and schools who use the Internet." 47 U.S.C. § 230(b)(3); Pet. App. 10a (Congress sought to increase internet security by "encourag[ing] the development of more sophisticated methods of online filtration." (citing H.R. Conf. Rep. No. 104-879, at 194 (1996))).

Those technologies have flourished in the ensuing years. Enigma's complaint identifies over 40 companies (including ESET) competing in this field. 2 CA9 ER 39. And many more enter the market each year.

But of course, not every company that claims to be dedicated to cyber security actually focuses on that end. Even though companies may describe their products as anti-malware or anti-virus software, that is often just a label. The use of such products can expose users to exploitation, lead users to falsely believe that their computer systems are secure, or simply cause users to waste time and money on worthless programs. This experience, in turn, can erode consumers' trust in security programs altogether, causing them to abandon efforts to secure their systems and leaving them vulnerable to future attacks.

The Ninth Circuit's decision hobbles efforts to develop filtering and blocking tools to combat such objectionable content. In doing so, the decision reduces internet security and stifles consumer choice.

I. The Ninth Circuit's Decision Undermines Internet Security by Deterring Development of Robust Blocking and Filtering Technologies and Decreasing Competition.

1. The CDA immunizes providers of interactive computer services from liability for making available the technical means to restrict access to objectionable material. 47 U.S.C. § 230(c)(2)(B). ESET and other cyber security companies can thus provide users a wide range of protections against online dangers and objectionable content, without the threat of a lawsuit from every disgruntled developer of an application identified as a potential problem.

Congress included no good-faith requirement for that immunity, unlike the immunity listed in the preceding provision. *Compare id. with* 47 U.S.C. § 230(c)(2)(A). Yet the Ninth Circuit created an implied exemption out of whole cloth, requiring courts to consider a company's motivation for providing users with the ability to restrict access to certain objectionable material.

Carving out an exception to the CDA's grant of immunity whenever a plaintiff alleges anticompetitive animus will interfere with Congress's goal of "remov[ing] disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b)(4). It will also hamper the equally important Congressional goal of "encourag[ing] the development of technologies which maximize user control over what information is received." 47 U.S.C. § 230(b)(3). By unsettling what was once a clear-cut

grant of immunity, the Ninth Circuit's decision discourages innovation—the exact opposite of what Congress intended.[3]

2. The decision below is an open invitation to purveyors of offensive, deceptive, objectionable, or useless material on the internet to write themselves an exception to the CDA immunity.

If the Ninth Circuit's opinion stands, anyone can manufacture a facially valid claim against a security software company simply by combining cyber security features with objectionable features. That's easy.[4] *See, e.g.*, *United States v. Microsoft Corp.*, 147 F.3d 935, 949 (D.C. Cir. 1998) (discussing how companies "bolt" unrelated software products together). Companies will then be able to claim, as Enigma does here, that any security software company that flags the

---

[3] The simplicity of the CDA's broad grant of immunity is what has allowed it to be such an effective force for technological innovation. *See* Derek Khanna, *The Law that Gave Us the Modern Internet—and the Campaign to Kill It*, The Atlantic (Sept. 12, 2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/ (explaining that the CDA "was simple and intuitive to understand for entrepreneurs and didn't require a lawyer to implement. As a result, it has functioned as a permission slip for the whole Internet that says 'Go innovate.'"). The decision below—which ignores the plain text of the CDA in favor of nebulous and ill-conceived policy considerations—undermines that essential clarity.

[4] *See, e.g.*, Steven Musil, *Cryptomining Malware Discovered Masquerading as Flash Updates*, CNET (Oct. 11, 2018, 6:00 AM), https://www.cnet.com/news/cryptomining-malware-discovered-masquerading-as-flash-updates/?ftag=CMG-01-10aaa1b (certain malware updates users' Adobe Flash program while also installing malicious cryptomining program).

product as potentially objectionable has acted with "anticompetitive animus"—simply because the product's maker has positioned itself as a competitor in the security software market.

This is not an abstract possibility. Programs that purport to be legitimate security software but in fact serve nefarious purposes have become "a major security threat."[5] Many of these programs operate in a "grey area," combining some security functionality with useless, annoying, or harmful features.[6] In a recent analysis of 250 purported antivirus apps in the Google Play store, for instance, less than a third of the apps were even functional; the rest were at best ineffective and at worst harmful.[7]

---

[5] Marco Cova et al., *An Analysis of Rogue AV Campaigns*, *in* RAID, *Recent Advances in Intrusion Detection* 442, 443 (Somesh Jha et al. eds., 2010); *see also* EC-Council, *Beware of Fake Anti-Virus Software*, EC-Council Blog (May 10, 2020), https://blog.eccouncil.org/beware-of-fake-antivirus-software/ (explaining that malicious "software that masquerades as a legitimate antivirus software . . . is one of the persistent threats on the web today").

[6] Hamish O'Dea, Virus Bulletin Conference, *The Modern Rogue – Malware with a Face* 209-210 (Sept. 2009), *available at* http://it.cc.stonybrook.edu/site_documents/index/news/rogue_malware.pdf; *see also* Juraj Malcho, Virus Bulletin Conference, *Is There a Lawyer in the Lab* 2-7 (Sept. 2009), *available at* https://www.virusbulletin.com/conference/vb2009/abstracts/there-lawyer-lab.

[7] AV Comparatives, *Android Test 2019* 3-6 (Mar. 2019), *available at* https://www.av-comparatives.org/tests/android-test-2019-250-apps/. Apps from ESET and Malwarebytes are both in the top tier—apps that detected at least 30% of malicious apps and had zero false alarms.

In addition, these programs often use deceptive marketing, distribution, and monetization tactics.[8] Such tactics include making false promises the program will provide complete security, using botnets to push installation onto a user's machine, and bundling "security" software with other dubious software that can slow down the system and make it more vulnerable to attack.

To combat these threats, legitimate cyber security companies must be able to provide tools that can filter or block objectionable content masquerading as a security program. *See, e.g.*, *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1170-71 (9th Cir. 2009) (defendant company's software blocked the plaintiff's "Spam Blocker Utility" as malware). But instead of fostering those efforts, the Ninth Circuit's decision allows purveyors of objectionable content to evade the CDA's immunity provisions just by positioning themselves as competitors.

3. Nor is the Ninth Circuit's decision workable. ESET's multilayered security programs encounter more than 300,000 new unique and suspicious objects *every day*. This threat landscape constantly shifts because of global events and the ingenuity of bad actors.[9] "Fighting modern malware is a cat-and-mouse

---

[8] *See* Malcho, *supra* n.6, at 2-7.

[9] *See, e.g.*, Jeremy Kahn, *Cybercriminals Adapt to Coronavirus Faster than the A.I. Cops Hunting Them*, Fortune (Apr. 30, 2020, 12:00 AM), https://fortune.com/2020/04/30/cybercriminals-adapt-to-coronavirus-faster-than-the-a-i-cops-hunting-them/; Lily Hay Newman, *Watch Out for Coronavirus Phishing Scams*, Wired Magazine (Jan. 31, 2020, 5:08 PM), https://www.wired.com/story/coronavirus-phishing-scams/.

game in which we face teams of skilled and (financially-) motivated bad guys."[10]

The only way to address such an onslaught is to employ technological tools that quickly scan and categorize new programs automatically, using "petabytes of intelligence gathered over many years by experienced researchers" to allow computers to predict which programs might be objectionable to users.[11] Legitimate security software companies can't review all content individually and give special deference to programs from entities that might later claim to be competitors.[12]

But the decision below opens the very real possibility that any purveyor of objectionable material subject to filtering might later claim to be a competitor and sue. This means that the more effective a provider makes its security software, the more vulnerable to litigation it becomes.[13]

---

[10] Jakub Debski et al., *ESET Technology: The Multilayered Approach and Its Effectiveness* 2 (v.1.3 2017), *available* at https://www.eset.com/us/business/resources/white-papers/eset-technology-the-multi-layered-approach-and-its-effectiveness-1/.

[11] *Id.* at 19.

[12] And even if this were possible, it would render users vulnerable to attacks from entities masquerading as competitors.

[13] Eric Goldman, *Online User Account Termination & 47 U.S.C. § 230(C)(2)*, 2 U.C. Irvine L. Rev. 659, 666 (Jun. 2012) (allowing suits to proceed based on naked allegations of subjective intent "gives plaintiffs the chance to hunt for evidence and imposes additional advocacy and discovery costs on the defendant"); *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008) (Section

When judicial decisions expand potential liability, the "invisible hand" of the free market will lead affected companies to avoid providing services that have become more legally risky.[14] *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 798 n.9 (9th Cir. 2007). Thus, although the decision below purports to serve procompetitive policy interests, it instead deters companies from developing effective filtering technologies. That reduces both the quality and quantity of competition in the legitimate cyber security software market.

The Ninth Circuit's decision hurts security software companies that try to provide users with effective means to screen out objectionable products. It benefits bad actors who can circumvent Section 230's immunity provisions to attack legitimate companies. It undermines Congress's goals of "encourag[ing] the development of technologies which maximize user control" and "remov[ing] disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b)(3), (4).

In sum, the perverse result of this decision will be to reduce the protection and choice that security companies can offer the public.

---

230 should provide protection "not merely from ultimate liability, but from having to fight costly and protracted legal battles.").

[14] A California state court recently rejected the Ninth Circuit's approach, concluding that it contradicted the plain text of the statute. *Prager Univ. v. Google LLC*, No. 19CV340667, 2019 WL 8640569 (Cal. Super. Ct. Nov. 19, 2019). The split between state and federal precedent on this issue—in the technology capital of the country—injects more legal uncertainty into the market.

II. The Ninth Circuit's Decision Defies Congressional Will by Substituting Litigation for Consumer Choice.

In its effort to protect Enigma from alleged anti-competitive animus, the Ninth Circuit seems to have forgotten that the whole purpose of Section 230(c)(2)(B) immunity is to maximize consumer choice. That choice should exist at two levels—when the consumer chooses which security product to use, and then again when the consumer chooses whether to remove objectionable materials. The Ninth Circuit's decision interferes with both choices.

1. Congress provided immunity to all providers of interactive computer services (like Malwarebytes, ESET, or their many competitors) for any action taken "to enable or make available to information content providers or others the technical means to restrict access to" objectionable material. 47 U.S.C. § 230(c)(2)(B).

That is, the security software company is not the party that restricts access. The company simply provides *its users* with the means to avoid objectionable products. The user decides whether to enable filtering of the potentially offending material, and the user can override the program's detection. Congress created immunity precisely to avoid fettering this consumer choice.

The upshot of the Ninth Circuit's decision is that a court should intervene between the security software company and the user to decide whether the company should be allowed to provide users with the technical means to restrict access to certain programs. Here, for example, the case is being remanded

to the district court to decide if Malwarebytes should have to pay civil damages for giving its users the ability to remove Enigma's program. Pet. App. 22a-23a. That will turn on a factual determination of whether Enigma's programs use "deceptive tactics," as Malwarebytes maintains, or instead "pose no security threat," as Enigma maintains. *Id*.

This judicial intervention is inimical to what Congress was trying to achieve in the CDA. "Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum." *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). Indeed, the statute opens with the express finding that "[t]he 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)(4).

2. Consumer choice also exists over which of the many available security software options to trust.

The internet is a dynamic marketplace, alive with almost instantaneous expert reviews, customer feedback, and social media communications. Congress expressly recognized that internet services "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." 47 U.S.C. § 230(a)(2). A security software company whose offerings serve its own interests to the detriment of its users' interests risks immediate exposure and the attendant consequences in the marketplace.

This reality underscores the fallacy of the Ninth Circuit's fundamental premise: that "interpreting the

statute to give providers unbridled discretion to block online content would . . . enable and potentially motivate internet-service providers to act for their own, and not the public, benefit." Pet. App. 20a. The free market drives providers to be better than their rivals at serving the interests of consumers. That is why Congress identified one of the cornerstone purposes of the CDA as "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[.]" 47 U.S.C. § 230(b)(2).

Rather than trust consumers to choose, as Congress did in enacting the CDA, the Ninth Circuit requires a court to make choices for consumers. The decision gives unscrupulous companies a weapon against legitimate cyber security providers, forcing legitimate providers to spend their resources fighting in court instead of developing the security products consumers want and need. That substitutes litigation for individual choice, frustrates competition, and harms consumers.

CONCLUSION

The Ninth Circuit's decision undermines Congress's goals in enacting the CDA, interferes with the development of programs to filter out objectionable online content, and limits consumer choice by interposing litigation as a barrier between the providers of security software and their users. Amicus ESET urges the Court to grant certiorari to address these issues of exceptional importance.

Respectfully submitted,

ANNA-ROSE MATHIESON
Counsel of Record
Susan Yorke
CALIFORNIA APPELLATE LAW GROUP LLP
96 Jessie Street
San Francisco, CA 94105
(415) 649-6700
annarose@calapplaw.com

June 2020