Appeal No. 17-17351

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ENIGMA SOFTWARE GROUP USA, LLC,
Plaintiff-Appellant,

v.

MALWAREBYTES, INC.,
Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA, NO. 5:17-CV-02915-EJD
THE HONORABLE EDWARD J. DAVILA, JUDGE

BRIEF OF ESET, LLC AS *AMICUS CURIAE* IN SUPPORT OF MALWAREBYTES' PETITION FOR PANEL REHEARING AND REHEARING EN BANC

ANNA-ROSE MATHIESON
CHARLES KAGAY
CALIFORNIA APPELLATE LAW GROUP LLP
96 JESSIE STREET
SAN FRANCISCO, CALIFORNIA 94105
TELEPHONE: (415) 649-6700

Attorneys for Amicus Curiae ESET, LLC

CORPORATE DISCLOSURE STATEMENT

ESET, LLC is a wholly owned subsidiary of ESET, spol. s r.o. No publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

INTEREST OF THE AMICUS

Amicus ESET, LLC is an award-winning computer security company driven by advanced research and development.[1] 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 and choice in their internet experience, and to build a more secure digital world in which everyone can enjoy safer technology.

ESET submits this amicus brief in the spirit of that mission. ESET sells computer security software and is a direct competitor to petitioner Malwarebytes, Inc. Yet while ESET normally competes vigorously with Malwarebytes, this case involves a question of such exceptional importance that ESET takes the unusual step of filing an amicus brief in support of one of its direct competitors. Unless the decision of the panel majority is reconsidered, ESET's goal—providing users the means to make their own choices about how to avoid objectionable materials—will become more difficult, and the internet will become a more dangerous and confusing place for consumers.

---

[1] All parties have consented to the filing of this amicus brief. Amicus certifies that no party or party's counsel authored the brief in whole or in part; that no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and that no person—other than the amicus and its counsel—contributed money that was intended to fund preparing or submitting the brief.

SUMMARY OF THE ARGUMENT

The majority opinion in this case undermines internet security and harms consumer choice in at least two critical ways.

First, the opinion creates a major roadblock to effective computer security software. The decision undercuts statutory immunity for filtering technology whenever there are allegations of anticompetitive animus, even though a purveyor of objectionable material can easily position itself as a competitor and make a facially plausible claim of such animus. This undermines Congress's goals in enacting the Communications Decency Act, 47 U.S.C. § 230 (1996) (CDA), and harms the procompetitive interests the majority opinion purports to protect.

Second, the decision substitutes litigation for the user choice that has created a thriving marketplace of protections available to consumers. 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 majority opinion would substitute litigation in which the user has no role for both of these choices.

The petition for rehearing in this case explains in detail why en banc consideration is necessary to secure uniformity of this Court's decisions, and ESET agrees. In particular, review is warranted because this issue is exceptionally important: As Congress has recognized,

Americans are becoming increasingly reliant on interactive media for political, educational, cultural, and entertainment services (47 U.S.C. § 230(a)(5)), but this decision will frustrate efforts to safeguard such use. Amicus ESET urges the Court to grant rehearing, either by the panel or en banc, to address these urgent issues.

ARGUMENT

Congress passed the CDA in part "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet . . . ." 47 U.S.C. § 230(b)(3). More specifically, Congress sought to increase internet security by "encourag[ing] the development of more sophisticated methods of online filtration." *Enigma Software Grp., USA, LLC v. Malwarebytes, Inc.*, 938 F.3d 1026, 1032 (9th Cir. 2019), citing H.R. Conf. Rep. No. 104-879, at 194 (1996). At this, the Act has surely succeeded. Enigma's complaint identifies over 40 companies (including ESET) competing in this field. ER 39. And many more enter the market each year.

But of course, not every company that claims to be dedicated to internet security is actually focused on that end. While Enigma's complaint in this case attempts to cast this as a business dispute between two competitors who make similar products, some software providers are

not transparent about their practices. Even though products may be labeled as anti-malware or anti-virus software, in many cases that is just a label. The use of such products can expose users to exploitation, lead users to falsely believe that their computer systems are properly secured, or simply cause users to waste time and money on worthless programs.

As a result, if the panel's decision in this case is allowed to stand, the result will be a reduction in internet security and consumer choice.

I. The majority opinion undermines internet security by affording purveyors of objectionable programs almost boundless opportunities to evade the Communications Decency Act's immunity provisions

At the outset, the fundamental notion behind this lawsuit—that one of the 40-plus competing security software companies could gain a competitive advantage by discouraging the use of the products of one of the others—is simply unfounded. " 'To have an "anticompetitive effect," conduct "must harm the competitive process and thereby harm consumers .... [H]arm to one or many competitors will not suffice." ' " *Spanish Broad. Sys. of Fla., Inc. v. Clear Channel Commc'ns, Inc.*, 376 F.3d 1065, 1071-72 (11th Cir. 2004), quoting *United States v. Microsoft Corp.*, 253 F.3d 34, 58 (D.C. Cir. 2001); *Dickson v. Microsoft Corp.*, 309 F.3d 193, 206 (4th Cir. 2002). "If a market contains many competitors, reducing that number by one . . . is unlikely to have any significant

anticompetitive effect . . . .” *W.T. Rogers Co., Inc. v. Keene*, 778 F.2d 334, 341 (7th Cir. 1985).

The CDA encourages the protection of internet users by immunizing providers of interactive computer services from liability for restricting (in good faith) access to objectionable material, and for enabling or making available (without regard to good faith) the technical means to restrict access to objectionable material. 47 U.S.C. § 230(c)(2)(A), (B). As the Court is well aware, it is the latter immunity at issue in the present case. That immunity allows computer security companies like ESET to develop and make available to users a wide range of protections against a daily onslaught of online dangers and objectionable content, without the threat of a lawsuit from the disgruntled developer of every application identified as a potential problem.

Carving out an exception to the CDA’s grant of immunity whenever a plaintiff alleges anticompetitive animus won’t advance Congress’s goal of “ ‘removing disincentives for the utilization of blocking and filtering technologies.’ ” *Enigma*, 938 F.3d at 1037, quoting 47 U.S.C. § 230(b)(4). And the panel’s decision will work to defeat an equally important Congressional goal: “to encourage the development of technologies which

maximize user control over what information is received . . . ." 47 U.S.C. § 230(b)(3).

The majority opinion in this case is an open invitation to purveyors of offensive, objectionable, or useless material on the internet to write themselves an exception to the CDA immunity. The majority opinion suggests that these companies can create a facially valid claim against security software companies by simply combining computer security features with objectionable features—and that is an easy task. *See, e.g.*, *United States v. Microsoft Corp.*, No. CIV. A. 98-1232, 1998 WL 614485, at *12 (D.D.C. Sept. 14, 1998), quoting *United States v. Microsoft Corp.*, 147 F.3d 935, 949 (D.C. Cir. 1998) ("the Court must determine whether Microsoft 'metaphorically "bolt[ed]" two products together,' 'for an anticompetitive purpose (or for no purpose at all).' ") Companies will then be able to claim, as Enigma does here, that any security software company that flags its product as a potentially unwanted application has acted with "anticompetitive animus" —simply because the maker of that application has positioned itself as a competitor in the security software market.

This is not an abstract possibility. The majority opinion attempts to distinguish this case from *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009)—in which this Court recognized that the CDA

shields a security software company from liability for blocking objectionable software—on the ground that "the parties in that case were not competitors," while "here the parties are competitors." *Enigma*, 938 F.3d at 1036, 1030. In fact, though, Zango sued Kaspersky, the defendant in that case, for blocking as malware a program Zango called "Spam Blocker Utility." 568 F.3d at 1170. A program that blocks spam is in direct competition with Kaspersky, ESET, and the more than 40 other companies in the security software field. If all that a malware purveyor need do to negate the CDA's immunity provisions is to purport to offer a component that filters out objectionable material, then the present case has effectively written *Zango* off the books.

Looking at the problem from the opposite perspective, there is no means by which a legitimate security software company can review individual purveyors separately and pay special heed to those that might later claim to be their competitors. ESET's multilayered security protects Windows, Mac, and Android devices from more than *a million attacks every day*. ESET's programs encounter more than 300,000 new unique and suspicious objects every day. The only way to address such an onslaught is to establish neutral criteria to advise internet users which programs appear to be objectionable; 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 majority opinion in this case 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.

The result is that a legitimate security software company, like ESET, will be faced with a strong disincentive to provide robust protections for its customers. If any purveyor of objectionable content is able to present a facial claim to being its competitor, then the security company will be faced with the strong possibility of expensive litigation simply for flagging objectionable content for the user to potentially remove. As this Court has recognized, when judicial decisions expand potential liability, the affected companies will be guided by the market's "invisible hand" to avoid providing services that have become more legally risky. *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788, 798 n.9 (9th Cir. 2007).

This cannot be what Congress meant when it sought "to encourage the development of technologies which maximize user control" and "to remove disincentives for the development and utilization of blocking and filtering technologies." 47 U.S.C. § 230(b)(3), (4). Any filtering technology must by definition provide means by which some

objectionable products do not reach potential consumers. The present decision has put a target on the back of every security software company, like Malwarebytes and ESET, whose very purpose is to provide users with the means to screen out objectionable products. The perverse effect of this decision will be to reduce the protection and choice that security companies can offer the public.

II. The majority opinion defies congressional will by substituting litigation for consumer choice

In its effort to protect Enigma from alleged anticompetitive animus, the majority opinion seems to have lost sight of the fact that the whole purpose of the CDA's Section 230(c)(2)(B) immunity is to maximize consumer choice. That section posits that no provider of an interactive computer service (like Malwarebytes, ESET, or their many competitors) will be held liable for any action taken "to enable or make available to information content providers or others the technical means to restrict access to" objectionable material.

That is to say, the security software company is not the party that restricts access. The company simply provides *the user* with the means to avoid objectionable products. The user decides whether or not 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 majority decision is that a court should intervene between the security software company and the user to decide whether the technical means the company has provided are acceptable. Here, for example, the case is being remanded to the district court for a factual determination of whether Enigma's programs use "deceptive tactics," as Malwarebytes maintains, or instead "pose no security threat," as Enigma maintains. *Enigma*, 938 F.3d at 1037-38.

This intervention is inimical to what Congress was trying to achieve through 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).

Congress's decision to minimize government intervention does not mean that consumer choice will be thwarted. In the end, the consumer decides which of the many available security software options to trust. *See, e.g.*, *Zango,* 568 F.3d at 1176:

> By providing its anti-malware software and malware definition update services, Kaspersky both enables and makes available the technical means to restrict access to malware. Users choose to purchase, install, and utilize the Kaspersky software.

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 majority opinion'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." *Enigma*, 938 F.3d at 1036. In a free market, providers acting in their own self-interest are driven by market forces to be better than their rivals at serving the interests of consumers. It was for this very reason that 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).

Instead of trusting to consumer choice, as Congress did in enacting the CDA, the majority opinion interposes a court to make choices for the consumer. The decision gives unscrupulous companies a weapon against legitimate internet security providers, thereby forcing companies to expend their resources in court battles instead of vigorously competing to offer the best internet security product. A rule of law that substitutes litigation for consumer choice frustrates rather than advances the procompetitive policies that the majority opinion claims to embrace.

CONCLUSION

The majority opinion in the present case undermines Congress's goals in enacting the CDA, interferes with the development of software 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 rehearing to address these issues of exceptional importance.

Respectfully Submitted,

Date: November 7, 2019

By: *s/ Anna-Rose Mathieson*

Anna-Rose Mathieson
Charles Kagay
California Appellate Law Group LLP

Attorneys for Amicus ESET, LLC

CERTIFICATE OF COMPLIANCE

Counsel for Amicus ESET, LLC certifies:

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 29(a)(5). This brief contains 2,563 words.

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the typestyle requirements of Federal Rule of Appellate Procedure 32(a)(6). This brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

Respectfully Submitted,

Date: November 7, 2019

By: *s/ Anna-Rose Mathieson*

Anna-Rose Mathieson
Charles Kagay
California Appellate Law Group LLP

Attorneys for Amicus ESET LLC

CERTIFICATE OF FILING AND SERVICE

I hereby certify I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the CM/ECF system on November 7, 2019. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system, which constitutes service pursuance to Federal Rule of Appellate Procedure 25(c)(2) and Ninth Circuit Rule 25-5(g).

Respectfully Submitted,

Date: November 7, 2019

By: *s/ Anna-Rose Mathieson*

Anna-Rose Mathieson
Charles Kagay
California Appellate Law Group LLP

Attorneys for Amicus ESET, LLC