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
Case No. 5:17-cv-02915-EJD
Honorable Edward J. Davila, District Court Judge

BRIEF OF AMICI CURIAE CYBERSECURITY LAW PROFESSORS IN SUPPORT OF MALWAREBYTES, INC.'S PETITION FOR REHEARING AND REHEARING EN BANC

VENKAT BALASUBRAMANI
FOCAL PLLC
900 First Ave. S, Ste. 201
Seattle, WA 98134
Fax: (206) 260-3966
Email: venkat@focallaw.com

ERIC GOLDMAN
PROFESSOR, SANTA CLARA
UNIVERSITY SCHOOL OF LAW
500 El Camino Real
Santa Clara, CA 95053
Tel: (408) 554-4369
Email: egoldman@gmail.com*

* *Santa Clara University School of Law 2L Jess Miers assisted with the preparation of this brief*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the undersigned states that none of the amici are corporations that issue stock or have a parent corporation that issues stock.

Dated: November 7, 2019

By: /s/ Venkat Balasubramani
Venkat Balasubramani

STATEMENT OF COMPLIANCE WITH RULE 29

This brief is submitted pursuant to Rule 29(b) of the Federal Rules of Appellate Procedure and Circuit Rule 29-2(a). In accordance with Federal Rule of Appellate Procedure 29(b) and Circuit Rule 29-2(a), counsel states that counsel for all parties have given consent to the filing of this amicus brief.

As required by Rule 29(a)(4)(E) of the Federal Rules of Appellate Procedure, counsel certifies that: no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief; and no person or entity—other than amici curiae, their members, or their counsel—contributed money that was intended to fund the preparation or submission of this brief.

Dated: November 7, 2019

By: /s/ Venkat Balasubramani
Venkat Balasubramani

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

IDENTITY AND INTERESTS OF AMICI

This brief of amici curiae is submitted on behalf of the following individuals (affiliations are for identification only):

Prof. Roger Allan Ford, University of New Hampshire Franklin Pierce School of Law

Prof. Yvette Joy Liebesman, Saint Louis University School of Law

Prof. Phil Malone, Juelsgaard Intellectual Property and Innovation Clinic, Stanford Law School

Prof. Connie Davis Nichols, Baylor Law

Riana Pfefferkorn, Center for Internet and Society, Stanford Law School

Prof. Rebecca Tushnet, Harvard Law School

Prof. Jonathan Weinberg, Wayne State University Law School

Amici are cybersecurity law professors and scholars who teach and write about the threats facing businesses and consumers online and how to combat those threats. Amici write to express their concerns about how the panel decision will benefit malefactors and undermine cybersecurity. Unless the Court corrects the panel decision, the amici are concerned that the decision will make the Internet less safe.

I. INTRODUCTION

The panel or the Court en banc should rehear this case so that it can reevaluate the ruling's consequences for cybersecurity. Though anti-competitive animus could be a troubling reason for one software program to block another, the Court's decision overcorrects for this concern. The panel decision will foster spurious legal accusations of anti-competitive blocking of software programs that are, in fact, dangerous to businesses and consumers. These legal threats will hinder the ability of anti-threat software vendors to properly classify threats to businesses and consumers, which will make the Internet less safe for everyone.

II. ARGUMENT

Businesses and consumers rely on third-party software to protect their computing devices from external threats. We refer to these third-party software providers as "anti-threat software vendors." The threats they manage include:

- Malicious software ("malware"), including spyware, ransomware, and viruses.

- Software that is not inherently pernicious but nevertheless may cause problems for users, sometimes called "Potentially Unwanted Programs" or "PUPs." These programs are also sometimes called "crapware" and can include adware and "bloatware."
- Unwanted content, such as spam or objectionable content.

Without robust anti-threat software, businesses and consumers would be overrun by threats that would render their computing devices unusable and expose them to financial, physical, and other risks. Any legal or regulatory scheme that undermines the ability of anti-threat software vendors to protect consumers and businesses poses a major threat to the Internet's integrity. *See generally* Roger Allan Ford, *Data Scams*, 57 HOUSTON L. REV. 111 (2019) (discussing the vital role that intermediaries play in combating online threats).

A. The Importance of Section 230(c)(2)(B)'s Safe Harbor

For more than two decades, 47 U.S.C. § 230(c)(2)(B) ("Section 230(c)(2)(B)") has provided a crucial legal foundation for the anti-threat software industry. Section 230(c)(2)(B) provides a safe harbor for anti-threat software vendors that protects their decision to classify software and content as "threats." In *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d

1169, 1176 (9th Cir. 2009), this Court interpreted Section 230(c)(2)(B) to give substantial deference to classification decisions by anti-threat software vendors.

Because of the *Zango* ruling and the broad applicability of Section 230(c)(2)(B), lawsuits over classification decisions have been rare in the past decade. As this Court said in *Zango*, the policy of "removing disincentives for the development of software that filters out objectionable or inappropriate material[] is served by a safe harbor for providers of malware-filtering software." *Zango*, 568 F.3d at 1174. The *Zango* ruling has successfully advanced that policy for the past decade.

The panel decision upends this legal foundation for the anti-threat software industry. It empowers malefactors to challenge an adverse classification decision as driven by anti-competitive animus, making anti-threat software vendors defend their decisions in court or bend their standards to avoid litigation. As anti-threat software vendors respond to the chilling effects of threatened litigation, more illegitimate software will reach businesses and consumers instead of being blocked. Furthermore, the increased costs to document and defend their classification decisions will be fatal to some anti-threat software

vendors, reducing consumer choice and counterproductively increasing the market power—and costs borne by businesses and consumers—of the few larger vendors who can survive.

B. Carving Out Allegations of "Anti-Competitive Animus" from Section 230(c)(2)(B) Benefits Rogue Software Vendors

At first blush, it might seem unusual for an anti-threat software vendor to label any rival anti-threat software program as a "threat." Because the vendors are marketplace rivals (at least nominally), intuitively any such negative classifications seem like they would be due to anti-competitive animus.

In reality, there are many legitimate reasons for anti-threat software vendors to make negative classifications of rivals.

First, well-known and well-regarded anti-threat software programs sometimes do not adequately protect businesses and consumers. For example, in 2016, Symantec's well-known Norton Anti-Virus program had critical security vulnerabilities that left its users exposed. *Symantec and Norton Security Products Contain Critical Vulnerabilities*, National Cyber Awareness System Alert (TA16-187A), Cybersecurity and Infrastructure Security Agency (CISA), July 5, 2016, https://www.us-cert.gov/ncas/alerts/TA16-187A. Separately, the well-

known McAfee "Security Suite" program has been labeled "crapware" because it unexpectedly slows down users' computers. Eric Griffith, *How to Rid a New PC of Crapware*, PCMAG (Feb. 7, 2018), https://www.pcmag.com/article/332543/how-to-rid-a-new-pc-of-crapware. Although these software programs are from well-established providers, they nevertheless may be "PUPs" to businesses and consumers. As a result, rival anti-threat software programs might label them as threats for legitimate—not anti-competitive—reasons.

Second, many programs that claim to be anti-threat software are actually the opposite—they create threats for businesses and consumers rather than provide protection from threats. There are many colloquial labels for anti-threat software programs that themselves pose threats to cybersecurity, including "scareware" and "fraudware." We call these programs "rogue software."

Rogue software can expose businesses and consumers to significant cybersecurity risks. Rogue software sometimes creates minor annoyances, like slowing down a user's computing device or displaying annoying popup ads. Rogue software can fleece consumers by demanding money to fix a problem that may not exist at all or that the

software program created itself. *See generally* Brett Stone-Gross et al., *The Underground Economy of Fake Antivirus Software*, June 1, 2011, https://escholarship.org/uc/item/7p07k0zr. In the worst cases, rogue software can create huge and potentially life-changing problems, like exfiltrating highly sensitive confidential data for criminal purposes.

There have been substantial litigation efforts to curb the abuses of rogue software vendors. Some examples:

Enforcer	Example Enforcements
Federal Trade Commission	• $163 million judgment against "scareware" marketer[1] • $35 million settlement with major retailer Office Depot for offering a software program that claimed to scan users' computers for viruses and other threats but, in fact, falsely reported that their computers had "malware symptoms" that could be "fixed" by paying for additional services[2]

[1] *FTC Case Results in $163 Million Judgment Against "Scareware" Marketer*, Federal Trade Commission (Oct. 2, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-case-results-163-million-judgment-against-scareware-marketer.

[2] *Office Depot and Tech Support Firm Will Pay $35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services*, Federal Trade Commission (Mar. 27, 2019),

State Attorneys General	• $1 million settlement for "marketing software that falsely claimed computers were infected with spyware, then enticing consumers to pay for a program that claimed to remove it"[3] • Defendants promoted their products by "misrepresenting that a consumer's computer is at risk [and] installing software without the computer user's consent"[4]
Private Plaintiffs	• Class action settlement for software that "provided potential customers with a free diagnostic scan designed 'to misrepresent and exaggerate the existence and severity of

https://www.ftc.gov/news-events/press-releases/2019/03/office-depot-tech-support-firm-will-pay-35-million-settle-ftc.

[3] *Attorney General McKenna Announces $1 Million Settlement In Washington's First Spyware Suit*, Washington State Attorney General Press Release (Dec. 4, 2006), https://www.atg.wa.gov/news/news-releases/attorney-general-mckenna-announces-1-million-settlement-washington-s-first.

[4] *Judge Finds Internet Affiliate Advertisers Violated Washington Spyware Law*, Washington State Attorney General Press Release (May 2, 2008), https://www.atg.wa.gov/news/news-releases/judge-finds-internet-affiliate-advertisers-violated-washington-spyware-law.

	detected errors, as well as the overall status of the PC"[5]

As these cases suggest, government enforcement and private litigation play a critical role in combating rogue software. However, those enforcement efforts are insufficient to protect businesses and consumers from these threats. Instead, businesses and consumers must rely on anti-threat software vendors as their primary defense against rogue software.

The panel decision undermines the ability of anti-threat software vendors to perform their vital functions. Rogue software vendors will regularly assert unsupportable claims that they are being negatively classified because of anti-competitive animus, not because they legitimately pose a threat to businesses and consumers. Without Section 230(c)(2)(B) to protect their classification decisions, anti-threat software vendors will spend more money defending their decisions. Or, in the face of challenges to their classification decisions, anti-threat software vendors will try to save money by avoiding a courtroom fight

[5] *Lagarde v. Support.com, Inc.*, No. C12-0609 JSC, 2013 U.S. Dist. LEXIS 42725, at *3 (N.D. Cal. Mar. 25, 2013).

and revising their classification. Neither outcome benefits businesses and consumers, but these outcomes will be the inevitable result of the panel decision—which allows rogue software programs to bypass the Section 230(c)(2)(B) safe harbor simply by claiming to be a victim of anti-competitive animus. Thus, the panel decision conflicts with the policy considerations that Section 230(c)(2)(B) was designed to advance.

III. CONCLUSION

In *Zango*, this Court explained that "[r]ecourse to competition is consistent with the statute's express policy of relying on the market for the development of interactive computer services." *Zango*, 568 F.3d at 1177. Competition has the best chance of thriving if anti-threat software vendors are free to do what they do best, without distortion from unfounded claims of anti-competitive animus made by vendors of rogue software.

The panel decision hampers anti-threat software vendors from performing their core functions of protecting consumers and businesses online. Because the ruling jeopardizes cybersecurity and makes all of us less safe, the panel or the Court en banc should review its decision.

Respectfully submitted and dated:

November 7, 2019

By: /s/ Eric Goldman
/s/ Venkat Balasubramani

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Circuit Rule 29-2(c)(2) and Fed. R. App. P. 32(f), I certify as follows:

1. This brief complies with the type-volume limitation because this brief is 10 pages and 1584 words (as calculated using the word count function of Microsoft Word), excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5)(A) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word, the word processing system used to prepare the brief, in 14-point Century Schoolbook font.

Dated: November 7, 2019 By: /s/ Venkat Balasubramani
Venkat Balasubramani

CERTIFICATE OF SERVICE

I hereby certify that on November 7, 2019, I electronically filed the foregoing brief of amici curiae with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: November 7, 2019 By: /s/ Venkat Balasubramani
Venkat Balasubramani