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 *AMICI CURIAE* CYBERSECURITY EXPERTS IN SUPPORT OF PETITIONER

Phillip R. Malone
Counsel of Record
JUELSGAARD INTELLECTUAL
PROPERTY AND
INNOVATION CLINIC
MILLS LEGAL CLINIC AT
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 725-6369
pmalone@stanford.edu

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Bruce Schneier, *Three Lines of Defense Against Ransomware Attacks by Cybercriminals*, N.Y. DAILY NEWS (MAY 15, 2017), https://perma.cc/RSS4-RGQK 10

Catalin Cimpanu, *Symantec, ESET, McAfee Rank First in Windows Anti-Malware Market Share*, ZDNET (Nov. 18, 2019), https://perma.cc/N5RQ-D72V 7

CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, *Protecting Against Malicious Code*, U.S. DEP'T HOMELAND SEC. (last revised Apr. 11, 2019), https://perma.cc/P2N7-A6PW 9

CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, *Symantec and Norton Security Products Contain Critical Vulnerabilities, National Cyber Awareness System Alert (TA16-187A)*, U.S. DEP'T HOMELAND SEC. (July 5, 2016), https://perma.cc/MZ53-A6P5 7

Eric Griffith, *How to Rid a New PC of Crapware*, PCMAG (Apr. 1, 2020), https://perma.cc/5497-8TGT 7

Evan Engstrom, *Primer: Value of Section 230*, ENGINE (Jan. 2019), https://perma.cc/N7C8-QSAY 15

FED. TRADE COMM'N, *FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams* (May 12, 2017), https://perma.cc/D624-JK3A 8, 9

FED. TRADE COMM'N, *How to Spot, Avoid and Report Tech Support Scams*, https://perma.cc/76K3-JNPF (archived June 1, 2020) 9

INTEREST OF *AMICI CURIAE*

Amici are cybersecurity experts who study, teach, and write about online threats and how to combat them.[1] *Amici* include law and computer science professors, researchers, and technologists.[2] *Amici* are concerned that the Ninth Circuit's decision creates a new and unprecedented exception to the legal immunity provided by 47 U.S.C. § 230(c)(2)(B) ("Section 230(c)(2)(B)") that will undermine cybersecurity. They join this brief because they believe that, unless this Court grants certiorari and corrects that decision, Internet users will be less safe.

SUMMARY OF ARGUMENT

This case involves a narrow legal issue with broad and exceptionally important implications for cybersecurity. The Ninth Circuit's ruling will expose Internet users to an array of threats that can compromise their systems and data, corrupt or extract their files, bog down their computers or smartphones, and weaponize their devices against other Internet users.

The decision below erodes the legal immunity provided by Section 230(c)(2)(B), which allows companies to develop robust anti-threat software to protect Internet users. In place of that immunity, the

[1] Parties' counsel were given timely notice of *amici's* intent to file this brief pursuant to Rule 37.2(a). The parties have consented to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund its preparation or submission. No person, other than *amici* or their counsel, made a monetary contribution to the preparation or submission of this brief.

[2] *Amici*'s names and affiliations are listed in Appendix A.

decision creates an opening for expensive and prolonged litigation. To avoid costly litigation and reduce business risk, anti-threat software vendors will opt to become overly conservative in identifying and blocking potential threats. This will leave tens of thousands of government entities, tens of millions of businesses, and hundreds of millions of Internet users more vulnerable to hazardous software.

The proper interpretation of Section 230(c)(2)(B) is an important federal question that has not been settled by this Court. Because the Ninth Circuit's interpretation will compromise the safety and security of Internet users, this Court should grant the petition for a writ of certiorari.

ARGUMENT

I. Anti-Threat Software Is Essential to Cybersecurity

Individual computer users and businesses are at risk of attack by online threats any time they are connected to the Internet.[3] Commercial anti-threat software, often colloquially referred to as "antivirus software," protects individuals and businesses from these threats and associated harms.

[3] All devices that access the Internet are at risk of attack, including desktop computers, laptops, tablets, and smartphones. Joshua Franklin et al., *Guidelines for Managing the Security of Mobile Devices in the Enterprise* v (Draft NIST Special Publication 800-124 Revision 2, Working Paper, 2020), https://perma.cc/3J8C-4XBC.

A. Internet Users Face a Wide Range of Dangerous Online Threats

Each day, more than 350,000 new online threats are identified, and more than a billion malicious programs are in circulation. *Malware*, AV-TEST INST. https://perma.cc/CC9X-XS2W (archived June 1, 2020). There are three general categories of threats that anti-threat software identifies and blocks:

1. Malicious software ("Malware") – software intentionally designed to damage computers or networks, or otherwise compromise their security. Malware infects victims' computers and comprises computer viruses,[4] trojan horses,[5] spyware,[6] ransomware,[7] and scareware.[8] Malware represents roughly 90% of software-based threats targeting

[4] Computer viruses are malicious programs designed to spread from one computer to another. They can replicate and run themselves without a user's knowledge. *See Virus*, NAT'L INST. STANDARDS TECH. COMPUTER SEC. RESOURCE CTR. (NIST CSRC), https://perma.cc/R95V-4NPQ (archived June 1, 2020).

[5] Trojan horses are malicious programs that disguise themselves as benign programs. Unlike viruses, they are not capable of replicating or running themselves. *See Trojan Horse*, NIST CSRC, https://perma.cc/FH55-YR86 (archived June 1, 2020).

[6] Spyware surreptitiously collects and distributes data from a victim's computer. *See Spyware*, NIST CSRC, https://perma.cc/NG2G-58DT (archived June 1, 2020).

[7] Ransomware encrypts user files and only restores access if the user pays a ransom. Jennifer Cawthra et al., *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events* 2, (Draft NIST Special Publication 1800-26, Working Paper, 2020), https://perma.cc/AS5G-SDXZ.

[8] Scareware relies on social engineering to trick victims into purchasing unwanted or malicious software. *See* Neil J. Rubenking, *How to Avoid Scareware*, PCMAG (Nov. 26, 2018), https://bit.ly/2ACsRGP.

individuals and businesses. *Malware*, AV-TEST INST.

2. Potentially Unwanted Programs ("PUPs") – software that is not always pernicious but may still cause problems for users. PUPs often slow down a computer's speed, collect private information, or display ads. They sometimes also weaken security because they can contain or constitute entry points for malware, or because they provide hackers additional access points. PUPs are responsible for over 10% of software-based threats targeting individuals and businesses. *Id.*
3. Unwanted content, such as spam or other content the individuals or businesses have decided to restrict.

Threats such as these can cause massive economic harm and disruption if they are not detected and blocked. For example, in one of the largest data breaches in history, malware placed on Target's security and payments system stole 40 million customer credit card numbers. Michael Riley et al., *Missed Alarms and 40 Million Stolen Card Numbers: How Target Blew It*, Bloomberg (Mar. 17, 2014), https://perma.cc/PDT9-YELN. This malware was a type that could have been stopped by anti-threat software; in fact, Target's anti-threat software flagged the threat (but Target unfortunately ignored that flag). *Id.* Were anti-threat software vendors discouraged or chilled from robustly protecting users, we would see countless more incidents like this.

The financial cost of malware to businesses is staggering. Ransomware alone, not counting other types of malware, may have cost the U.S. more than $7.5 billion of damage in 2019. Patrick Howell O'Neill, *Ransomware May Have Cost the US More Than $7.5 Billion in 2019*, MIT TECH. REV. (Jan. 2, 2020), https://perma.cc/QXV6-9VER.

Meanwhile, malware attacks are rapidly increasing as a result of the ongoing COVID-19 pandemic. One illustration of the scope of this threat is that a single entity, Google's Threat Analysis Group, has reported detecting 18 million malware and phishing Gmail messages per day related to coronavirus. Shane Huntley, *Findings on COVID-19 and Online Security Threats*, GOOGLE THREAT ANALYSIS GROUP (Apr. 22, 2020), https://perma.cc/BU3S-QAL9. The Federal Bureau of Investigation's Internet Crime Complaint Center has received more than 3,600 complaints related to COVID-19 scams, many involving websites that distribute malware. *Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams*, U.S. DEP'T. JUST. (Apr. 22, 2020), https://perma.cc/8Z7P-2RRM. At the same time, hackers are using COVID-19 scams to gain access to corporate systems. James Rundle et al., *Hackers Target Companies with Coronavirus Scams*, WALL STREET J. (Mar. 4, 2020), https://perma.cc/9AU6-SFMN.

There have never been more, or more serious, online threats to cybersecurity.

B. "Rival" Anti-Threat Software Can Be a Genuine Threat

While hackers and other malefactors as the source of malware seems logical, there is another, counter-intuitive, reality: rival anti-threat software can in fact be a bona fide threat that needs to be blocked from users. There are two primary situations where that occurs. First, even well-known anti-threat software can create significant enough risks that its rivals may want to warn their users about it. Second, anti-threat software can be threatening or threat-creating software disguised as legitimate protective software. This is often called "rogue security software."

As an example of the former, in 2016, Symantec's flagship "Norton AntiVirus" software had critical security vulnerabilities that left its users exposed. *Symantec and Norton Security Products Contain Critical Vulnerabilities, National Cyber Awareness System Alert (TA16-187A)*, CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T HOMELAND SEC. (July 5, 2016), https://perma.cc/MZ53-A6P5.[9] Moreover, McAfee's "Security Suite" antivirus software is often pre-installed on computers and unexpectedly slows them down, leading observers to call it "crapware," a type of PUP. *See, e.g.*, Eric Griffith, *How to Rid a New PC of Crapware*, PCMAG (Apr. 1, 2020), https://perma.cc/5497-8TGT. Symantec and McAfee license the first and third most popular anti-threat software programs worldwide for Windows Operating Systems. Catalin Cimpanu, *Symantec, ESET, McAfee Rank First in Windows Anti-Malware Market Share*, ZDNET (Nov. 18, 2019), https://perma.cc/N5RQ-D72V.[10] Anti-threat software can drastically improve system performance by classifying bloated anti-threat software—by definition, from rival vendors—as a threat. *See* J. D. Biersdorfer, *Why One Antivirus Program Is Better Than Two*, N.Y. TIMES: TECH TIP (July 27, 2017), https://perma.cc/26JS-U2K9. That is precisely what Malwarebytes did in this case. *See* Pet. App. 12a-13a.

In the latter situation, rogue security software impersonates a legitimate anti-virus scanner, "detects" nonexistent malware or malware it installed

[9] Symantec has since rebranded as NortonLifeLock. *Symantec Completes Sale of Enterprise Security Assets to Broadcom*, NORTONLIFELOCK (Nov. 4, 2019), https://perma.cc/L8FD-G4SR.

[10] This figure excludes Microsoft's Windows Defender, which comes pre-installed with Windows.

itself, and displays fraudulent alerts to trick victims into purchasing the license for a "commercial version" of the software capable of "removing" the nonexistent or real security threat.[11] Brett Stone-Gross et al., *The Underground Economy of Fake Antivirus Software* 1 (U.C. Santa Barbara Dep't of Econ., Working Paper, 2011), https://perma.cc/A727-6K5S.

On their own, users are unlikely to recognize that rival anti-threat software can create security threats. For example, some creators of rogue security software have gone so far as to make fake customer service and technical support for their fraudulent products. *See id.* at 8; *FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams*, FED. TRADE COMM'N (May 12, 2017), https://perma.cc/D624-JK3A.

Thus, there will often be legitimate safety and security reasons for an anti-threat software vendor to classify rival anti-threat software as a threat. Such decisions do not inherently indicate anticompetitive animus or conduct.

C. Anti-Threat Software Offers Critical Protection Against Online Threats

Many individuals and businesses depend on anti-threat software as a primary defense against dangerous online threats. Murugiah Souppaya & Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* 11 (NIST Special Publication 800-83 Revision 1, Working Paper, 2013), https://perma.cc/T3D9-YCNT (recognizing that "antivirus software has become a necessity for malware incident prevention."). Both the Federal

[11] In other words, rogue security software is usually scareware. *See supra* note 8.

Trade Commission and the Department of Homeland Security recommend users install anti-threat software to safeguard their online experience. *Spyware and Malware*, FED. TRADE COMM'N, https://perma.cc/LW7T-PJWQ (archived June 4, 2020); *Protecting Against Malicious Code*, CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, DEP'T HOMELAND SEC., U.S. DEP'T HOMELAND SEC. (last revised Apr. 11, 2019), https://perma.cc/P2N7-A6PW.

Although federal and state enforcement actions and private class action lawsuits have attempted to curb malicious software abuses, *Crackdown on Tech Support Scams,* FED. TRADE COMM'N, litigation alone cannot sufficiently protect Internet users from the multitudinous and rapidly emerging online threats. Similarly, educating users to detect various scams can go a long way,[12] but scams are rapidly evolving and even savvy Internet users are tricked into downloading malware. pzdupe1, *Even This Expert on Hackers Got Tricked Into Clicking a Scam Email*, BUS. INSIDER (Aug. 9, 2016), https://perma.cc/F8LL-P6TM.

Thus, anti-threat software is essential. It can classify threats as PUPs or malware, blocking them from Internet users and thereby protecting those users from mistakenly accessing harmful content. Identifying and blocking harmful software is vital for fending off rogue security software, the creators of which go to great lengths to conceal the dangerous nature of their programs. *See* Stone-Gross et al., *Fake Antivirus Software*, at 2, 14. Anti-threat software can also catch Internet users' mistakes—for example, identifying when an employee has clicked on a file attachment that contains malware and preventing it from running. Bruce Schneier, *Three Lines of Defense*

[12] *See e.g.*, *How to Spot, Avoid and Report Tech Support Scams*, FED. TRADE COMM'N, https://perma.cc/76K3-JNPF (archived June 1, 2020).

Against Ransomware Attacks by Cybercriminals, N.Y. DAILY NEWS (MAY 15, 2017), https://perma.cc/RSS4-RGQK.

II. The Decision Below Erodes the Immunity That Anti-Threat Software Providers Have Relied Upon to Identify Threats and Protect Internet Users

In order to provide effective protection against pernicious online threats, anti-threat software vendors must be able to proactively and aggressively identify and block those threats. For more than two decades, Section 230(c)(2)(B) has provided the legal certainty anti-threat software vendors need to do just that. It grants these vendors immunity from most federal and state lawsuits for threat classification decisions. The Ninth Circuit's erroneous interpretation of Section 230(c)(2)(B) strips them of that immunity and reduces the legal certainty that has permitted them to fully protect Internet users.

Traditionally, anti-threat software vendors have been given strong deference over these classification decisions. The Ninth Circuit itself has recognized that Congress' explicit policy goal (as expressed in Section 230(b)(4)) 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 Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1174 (9th Cir. 2009). This reflects the reality that anti-threat software vendors are best equipped to identify evolving and emerging online threats.

Section 230(c)(2)(B) immunity has enabled these vendors to identify and block threats without constantly worrying that they will have to defend their identification and classification decisions in expensive litigation brought by those whose threats they block.

Section 230(c)(2)(B) immunity protections, which up to now have been consistent and clear-cut, have enabled vendors to avoid costly litigation and instead focus their resources on identifying threats and protecting users.

The decision below undermines this critical legal protection and creates a vulnerability in Section 230(c)(2)(B) that anti-threat software vendors will be unable to patch. It creates an exception to Section 230(c)(2)(B) immunity, found nowhere in the language of the statute, that would allow lawsuits challenging anti-threat vendors' decisions to classify and block software as threats. In so doing, it ignores how anti-threat software is designed and implemented, and disregards the importance of Section 230(c)(2)(B) in sustaining a healthy cybersecurity ecosystem.

It does so in two interrelated ways. First, it permits spurious legal claims based on mere allegations of "anticompetitive animus" by vendors whose products have been identified as threats. Second, it creates powerful disincentives for anti-threat software vendors to aggressively identify threats, thus undermining the safety and security of their users.

A. The Decision Below Allows Mere Allegations of Anticompetitive Animus to Upend Section 230's Immunity

Under the Ninth Circuit's erroneous interpretation of Section 230(c)(2)(B), for a plaintiff to strip an anti-threat software provider of Section 230 immunity, it need only allege that the decision to label its software as a threat was "driven by anticompetitive animus." Pet. App. 11a. A mere allegation will usually be sufficient to upend the legal certainty that has long permitted anti-threat providers to classify and respond to threats as they see best for their customers.

The providers' decisions about what threats to identify and guard against, no matter how well founded, can now be second guessed in expensive and burdensome litigation.

The disincentives created by eliminating certainty and exposing providers to costly lawsuits are much more significant than they might first appear. This new legal vulnerability can be leveraged not only by genuine rivals that offer comprehensive anti-threat software suites, like Enigma and Malwarebytes, but also by a far larger number of companies that hardly resemble them but that can make some credible claim to being rivals.

There are roughly 50 companies that offer comprehensive anti-virus suites to identify external threats, like Enigma and Malwarebytes. *The Best Antivirus Software for Android*, AV-TEST INST., https://perma.cc/8RK9-AMW7 (archived June 1, 2020). To illustrate the magnitude of the impact of the decision below, consider that each of these 50 players may classify the software of each rival, resulting in 10,000 classification decisions that can now potentially be challenged under the "anticompetitive animus" exception.[13]

But beyond these 50 players, there are likely hundreds of software companies that can sufficiently allege that they are "competing" anti-threat software vendors and escape having their lawsuits dismissed

[13] Among these 50 industry players, many have multiple product families. If each player has four anti-threat software products on the market, there are 50 x 49 x 4 = 9,800 classifications of each other's products the vendors must collectively make, since each vendor must make a classification decision about each of the other 49 vendors' four software products. Note that in this case, Enigma sued Malwarebytes over negatively classifying two different Enigma products, SpyHunter and RegHunter. Pet. App. 14a.

under the Ninth Circuit's new Section 230 exemption. These companies include creators of web browsers, advertisement blocking software, rogue security software, or any other program that legitimately or illegitimately scans the Internet or computers for malware or otherwise classifies other programs as threats.

Because so many different direct and indirect competitors could plausibly claim to create products that do this, it is difficult to put a number on how many vendors could take advantage of the decision below. But even an estimate of 500 unique software vendors, each with a single product on the market, would mean that nearly 250,000 threat classifications could be exempt from the protections of Section 230(c)(2)(B) under the Ninth Circuit's interpretation.[14] If even a fraction of those classifications resulted in lawsuits by even a fraction of the vendors whose products were classified as threats, this would open up the possibility of a dramatic number of new vendor-vs.-vendor lawsuits in an area that has up to now been predictable and seen little litigation.

B. The Threat of Costly Litigation Creates Powerful Disincentives for Anti-Threat Software Vendors to Classify and Block Threats

The Ninth Circuit's ruling will force anti-threat software vendors to divert precious resources away from developing the best possible products to protect their users. Instead, they will have to spend time and money assessing the litigation risks of classifying

[14] There would be 500 x 499 = 249,500 classification decisions, since each of the 500 software vendors would have to make a classification decision about each of the other 499 vendors' software products.

questionable software or content as a threat and defending against lawsuits challenging those classification choices. The result will be reduced protection for Internet users.

The Ninth Circuit has properly recognized Section 230 as "an immunity statute" that "protect[s] websites not merely from ultimate liability, but from having to fight costly and protracted legal battles." *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008). But under the decision below, mere allegations of anticompetitive animus will be sufficient to sidestep that immunity and expose anti-threat providers to precisely the sort of expensive and lengthy litigation the Ninth Circuit warned about. Low pleading standards at the motion to dismiss stage mean rivals will often be able to make credible if pretextual allegations of anticompetitive animus. After all, anticompetitive animus seems intuitively plausible when a threat classification is made against a direct or at least nominal rival. Spurious claims that previously would have been quickly blocked by Section 230(c)(2)(B) immunity will become a frequent—and costly—reality.

Since the decision below, there has already been at least one such case. In *Asurvio LP v. Malwarebytes Inc.*, No. 5:18-CV-05409-EJD, 2020 WL 1478345 (N.D. Cal. Mar. 26, 2020), the district court rejected a claim that the plaintiff in that case was a competitor of Malwarebytes when its allegedly competitive service was technical support for the removal of malware. While the district court reached the right result in this particular case, the lawsuit itself previews the kind of voluminous unmeritorious litigation heading for the court system because of the decision below.

The immunity from expensive and lengthy litigation that Section 230(c)(2)(B) provides is particularly important for smaller and newer anti-threat software providers, including innovative startups that rely on novel techniques and programs to detect malicious behavior and identify threats. Increased litigation costs can drive smaller players from the market. For an anti-threat software startup, having to litigate a case to the summary judgment stage, rather than ending it early as Section 230 immunity currently allows, can increase the cost of litigation between $15,000 and $150,000 per lawsuit (on top of the $15,000 to $80,000 it already costs to litigate to a motion to dismiss). Evan Engstrom, *Primer: Value of Section 230*, ENGINE (Jan. 2019), https://perma.cc/N7C8-QSAY. Without Section 230(c)(2)(B) immunity, some anti-threat companies, especially startups, will be forced out of the market. The result will be reduced competition, less innovation and consumer choice, and weaker safety and security for Internet users.

Anti-threat software vendors may seek to avoid the time, distraction, and expense required to litigate these new claims by pulling their punches and becoming more conservative in identifying and blocking threats from any firm that might plausibly claim to be a rival. As the Ninth Circuit explained in an earlier case, "there will always be close cases where a clever lawyer could argue that *something* the website operator did encouraged [] illegality." *Roommates.com*, 521 F.3d at 1174. For anti-threat software vendors, close cases are especially likely to involve rogue security software and PUPs.

Out of fear of litigation, these vendors may become hesitant to proactively classify rogue security software as PUPs or malware. Specifically, vendors may become more cautious in developing heuristics to flag rogue security software out of concern that they might inadvertently block legitimate rival software and end up embroiled in litigation.[15] Similarly, if rogue security software or PUPs are actually identified and blocked, and the rogue or PUP providers file suit, then anti-threat software vendors may opt to dispose of that litigation quickly by manually unflagging the software—even if the reclassification does a disservice to all of the vendor's users. To proactively avoid the potential threat of litigation, anti-threat software vendors likely will be chilled in their decision-making, prompting them to loosen their standards and refrain from classifying potentially dangerous software as threats.

In all of these circumstances, fewer bona fide threats to users will be identified and blocked. Ultimately, overcautious threat identification and classification caused by the loss of immunity will result in less-robust and less-effective anti-threat software.

The Ninth Circuit previously recognized that close cases involving Section 230 must be resolved in favor of immunity, "lest we cut the heart out of § 230 by forcing websites to face death by ten thousand duck-bites." *Roomates.com*, 521 F.3d at 1174. But the decision below forces anti-threat providers to face just that danger. It presents them with a devil's bargain—risk ruinous litigation or classify fewer dangerous software products as threats, which will weaken cybersecurity and leave the Internet ecosystem less secure.

[15] One of the major strategies anti-threat software employs is "heuristic analysis," which compares the behavioral patterns of suspected threats to those of known malicious software. If the behavior is similar, the program is blocked. Creating evolving and clever heuristics is particularly important to identifying novel malicious threats, but heuristics can lead to false positives. *See* TODD G. SHIPLEY & ART BOWKER, INVESTIGATING INTERNET CRIMES 157 (2014).

CONCLUSION

The decision below erroneously interprets the clear text of Section 230(c)(2)(B) and undermines its express policy goals. It purports to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services," as Congress intended. Pet. App. 47a; Section 230(b)(2). But in so doing, it endangers the competitive market for effective anti-threat software by creating an unprecedented opening for costly litigation.

The threat of that litigation will force anti-threat software vendors to divert precious resources away from protecting their customers or curtail their identification of dangerous threats, and it may drive some of them out of the market. Rather than "remov[ing] disincentives for the development and utilization of blocking and filtering technologies," *see* Section 230(b)(4), this ruling does the opposite. It creates new and unprecedented disincentives for developing and utilizing such technologies, putting our broader online safety and security at risk. *Id.*

This Court should grant the petition for a writ of certiorari to restore the proper interpretation of Section 230(c)(2)(B) and to eliminate the serious and immediate threats to cybersecurity posed by the Ninth Circuit's decision.

Respectfully submitted,

Phillip R. Malone
Counsel of Record
JUELSGAARD INTELLECTUAL
PROPERTY AND INNOVATION
CLINIC
MILLS LEGAL CLINIC AT
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 725-6369
pmalone@stanford.edu

June 12, 2020

APPENDIX A -- LIST OF AMICI

Amici curiae are listed below. Affiliation is provided for identification purposes only; all signatories are participating in their individual capacity and not on behalf of their institutions.

Dr. Richard Forno
University of Maryland Baltimore County

Professor Elizabeth Townsend Gard
Tulane University Law School

Professor Eric Goldman
Santa Clara University School of Law

Joseph Lorenzo Hall
Internet Society

Eran Kahana
Stanford Law School
CodeX—The Stanford Center for
Legal Informatics

Professor David S. Levine
Elon University School of Law

Professor Yvette Joy Liebesman
Saint Louis University School of Law

Professor Connie Davis Nichols
Baylor Law

David O'Brien
Berkman Klein Center for
Internet & Society at Harvard University

Professor Barak Orbach
The University of Arizona
James E. Rogers College of Law

Riana Pfefferkorn
Stanford Law School
Center for Internet and Society

Professor Jennifer M. Urban
University of California, Berkeley, School of Law

Professor Jim Waldo
Harvard John A. Paulson School of
Engineering and Applied Science
Harvard Kennedy School

Professor Jonathan Weinberg
Wayne State University