No. 19-1284

IN THE

# Supreme Court of the United States

MALWAREBYTES, INC,

*Petitioner,*

*v.*

ENIGMA SOFTWARE GROUP, USA,

*Respondent.*

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

## BRIEF OF ELECTRONIC FRONTIER FOUNDATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

SOPHIA COPE
*Counsel of Record*
AARON MACKEY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

*Attorneys for Amicus Curiae*

296228

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

## TABLE OF CONTENTS

*Table of Contents*

## TABLE OF CITED AUTHORITIES

*Cited Authorities*

*Page*

**Statutes**



**Other Authorities**

*Cited Authorities*

## INTERESTS OF *AMICUS CURIAE*[1]

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit civil liberties organization that has worked for 30 years to protect free speech, privacy, security, and innovation in the digital world. EFF, with over 30,000 members, represents the interests of technology users in court cases and broader policy debates surrounding the application of law to the Internet and other technologies.

## SUMMARY OF ARGUMENT

The Court should grant certiorari to correct a misreading of a key federal law that allows Internet users to customize their online experiences and protect themselves from objectionable and harmful material. The Ninth Circuit's decision below creates an exception in Section 230's unequivocal protection for the providers of online filtering tools—47 U.S.C. § 230(c)(2)(B)—that is unmoored from the plain language of the law and Congress' purpose in enacting it. The petition demonstrates why the Court must correct the error as a matter of straightforward statutory interpretation. EFF submits this *amicus curiae* brief to show how the Ninth Circuit's misreading of the law discourages the development of effective online filtering tools, to the detriment of Internet users.

---

1. 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 other than the *amicus curiae* or their counsel made a monetary contribution intended to fund the brief's preparation or submission. All parties have consented in writing to the filing of this brief.

Filtering tools give Internet users choices. People use filtering tools to directly protect themselves and to craft the online experiences that comport with their values, by screening out spyware, adware, or other forms of malware, spam, or content they deem inappropriate or offensive. Platforms use filtering tools for the same reasons, enabling them to create diverse places for people online. The Ninth Circuit's interpretation of Section 230(c)(2)(B) threatens the continued availability of these tools.

The Ninth Circuit's decision also seriously threatens an online tool *amicus* EFF has built that allows Internet users to stop advertisers and other third-party trackers from secretly tracking them as they browse the web. Public interest technologists have developed this free tool, called Privacy Badger, as part of a larger effort to empower Internet users to protect their privacy online.

Finally, the Ninth Circuit's misinterpretation of Section 230(c)(2)(B) makes it more challenging for EFF and others to continue to push filtering tool providers to block harmful software that is used to perpetuate domestic violence and harassment. EFF is working to eradicate this so-called "stalkerware," and that goal is more likely to be achieved when filtering tool providers have the unqualified Section 230(c)(2)(B) immunity that Congress intended. The Ninth Circuit's decision leaves filtering tool providers potentially subject to baseless claims that their efforts to eradicate stalkerware were undertaken for anticompetitive purposes, discouraging them from taking affirmative steps to eradicate this kind of harmful software.

## ARGUMENT

### I. The Plain Language of Section 230(c)(2)(B) Does Not Include an Anti-Competitive or Good Faith Exception

Congress enacted Section 230(c)(2)(B)'s broad immunity for filtering tool providers to ensure the widespread development of blocking software that would empower Internet users and service providers to control their online experiences. If Congress was concerned that filtering tool providers would abuse Section 230(c)(2)(B)'s unequivocal protection for anti-competitive purposes, it would have included a carve-out in the statute. That carve-out does not exist in the text, and the Ninth Circuit erred in adding one.

Sections 230(c)(2)(A)-(B) provide immunity from liability for filtering tool providers and Internet users that block content or products they deem objectionable. Section 230(c)(2)(B) states that "no provider or user of an interactive computer service shall be held liable on account of any action taken to enable or make available to information content providers or others the technical means to restrict access to material described" in Section 230(c)(2)(A). That includes "material that *the provider or user considers to be* obscene, lewd, lascivious, filthy, excessively violent, or otherwise objectionable." Section 230(c)(2)(A) (emphasis added). Section 230(c)(2)(B) thus provides immunity for the blocking of material that a provider or user deems to be objectionable or as otherwise described in Section 230(c)(2)(A). 47 U.S.C. § 230(c)(2)(A) & (B). The plain meaning of the provisions is that Section 230(c)(2)(B) immunizes the filtering tool providers'

*subjective* decisions about what content or products are objectionable under Section 230(c)(2)(A).

The Ninth Circuit ignored Section 230(c)(2)'s text to create a new exception to Section 230(c)(2)(B)'s immunity. The panel substituted its own determination of what counts as "objectionable" material per Section 230(c)(2)(A), rather than acknowledging that the statutory text provides immunity for blocking "material the provider or user considers" objectionable. There is no textual basis in Section 230(c)(2) to support the Ninth Circuit's conclusion that blocking a competitor's product allegedly based on an "anticompetitive animus" makes the blocked software *not* "objectionable" material under Section 230(c)(2)(A) and thereby removes Section 230(c)(2)(B)'s immunity. *See Enigma Software Group USA, LLC, v. Malwarebytes, Inc.*, 946 F.3d 1040, 1045, 1050 (9th Cir. 2019) (amended opinion).

By voiding statutory immunity when blocking allegedly occurred for an anti-competitive purpose, the Ninth Circuit panel effectively created a general "good faith" exception to the immunity granted to providers of filtering tools by Section 230(c)(2)(B). However, the *Enigma* panel's reading of a good-faith exception into Section 230(c)(2)(B) is contrary to the plain language of the subsection specifically and the statute as a whole. Although Section 230(c)(2)(A) does have an express good faith limitation, Section 230(c)(2)(B) does not. *See* 47 U.S.C. § 230(c)(2)(A) & (B).

Moreover, the rules of statutory interpretation counsel against reading such an exception into Section 230(c)(2)(B). "[W]here Congress includes particular language in one section of a statute but omits it in another section of

the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States*, 464 U.S. 16, 23 (1983) (internal quotations and citation omitted).

## II. Reading Any Exception Into Section 230(c)(2)(b) Immunity Harms Internet Users By Discouraging the Development and Use of Online Filtering Tools

Reading any exception into Section 230(c)(2)(B) ultimately harms Internet users. The Ninth Circuit's creation of an anti-competitive exception to Section 230(c)(2)(B) is on balance more harmful to Internet users than the panel's concern that giving broad immunity to filtering tool providers would allow them to stifle competition. *See Enigma Software Group USA, LLC*, 946 F.3d at 1051.[2] The Ninth Circuit's decision—by exposing filtering tool providers to new legal liability, as well as the costs and burdens of litigation—is likely to lead to Internet users having less robust and fewer filtering tools to choose from, disempowering them (and the platforms they use) from fashioning the online experiences that reflect their values.

### A. The Ninth Circuit's Decision Will Chill the Development of Online Filtering Tools

The *Enigma* panel's decision creates legal uncertainty for filtering tool providers that, in turn, promises to create a chilling effect to the detriment of Internet

2. In this case, as the *Enigma* panel suggested, if an Internet user already has Malwarebytes' filtering tool installed, and the user then attempts to download Enigma's products, the user is given a warning but may actually continue with the download. *Enigma Software Group USA, LLC*, 946 F.3d at 1047.

users. Should the decision stand, filtering tool providers will seek to minimize their legal exposure by creating weaker, less effective filtering tools for fear of sweeping in competitors—or otherwise doing something that could lead to allegations of acting in "bad faith." Additionally, some would-be entrepreneurs might not even take the chance on entering the filtering tool market in the first place.

This chilling effect flows not just from the fear of being held legally liable for a variety of causes of action, *but also from the fear of having to face costly and burdensome litigation*. Small filtering tool companies, in particular, may have difficulty shouldering the costs of litigation, in addition to ultimate liability. In this case, Enigma's allegations of "anticompetitive animus" on the part of Malwarebytes were sufficient to defeat a motion to dismiss. *Enigma Software Group USA, LLC*, 946 F.3d at 1045. This means that a filtering tool provider may, in fact, have acted in good faith by blocking a competitor, but it may be sued anyway via a plausibly alleged complaint, *see Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and would be required to defend itself through discovery, then summary judgment or trial—which are, of course, very long and costly legal proceedings.

Yet Congress intended Section 230 to provide immunities from suit as well as liability. *See* 47 U.S.C. § 230(e)(3) ("[n]o cause of action may be brought and no liability may be imposed"); *Fair Housing Counsel of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc) (holding that Section 230 cases "must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites"); *Hassell v.*

*Bird*, 5 Cal. 5th 522, 544 (2018) ; *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009) .

### B. Online Filtering Tools Can Inadvertently Flag False Positives, Which May Wrongly Be Used as a Basis for Claiming Providers Acted in Bad Faith

The risk of losing a motion to dismiss despite having acted in good faith is real given how online filtering tools function. Whether they screen out spyware, adware, or other forms of malware, spam, or unwanted content, online filtering tools operate by using two main methodologies. One involves the creation of block lists of known bad software, websites, or content, also called a "signature-based analysis." The other involves the use of heuristics or rules-based filtering.[3] In this case, Malwarebytes similarly uses rules or "criteria" to flag potentially problematic software. *Enigma Software Group USA, LLC*, 946 F.3d at 1047-48.

Thus, the first methodology implies deliberate action or an intent to block by the filtering tool provider. The second methodology, by contrast, may result in a competitor being flagged by the filtering tool, but this fact

3. See Karen Scarfone & Peter Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Special Publication 800-94, § 8.3.2, Nat'l Inst. of Standards & Tech. (NIST), U.S. Dept. of Commerce (Feb. 2007) ("Both antivirus and antispyware products detect threats primarily through signature-based analysis. To identify previously unknown threats, they also use heuristic techniques that examine activity for certain suspicious characteristics."), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

alone does not *prove* an allegation of an anti-competitive purpose. The flagging of a competitor may have been done inadvertently, for reasons unrelated to the fact that the company is a competitor.[4] Thus, false positives are possible, yet a filtering tool provider may be sued, lose a motion to dismiss, and be forced to carry on through discovery and a ruling on the merits in order to prove it acted in good faith.

### C. The FOSTA Fallout Illustrates the Risks of Creating New Exceptions to Section 230

The chilling effect that results from weakening any of Section 230's immunities is best illustrated by the far-reaching and harmful consequences to user speech that followed Congress' passage of the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) in 2018.[5] FOSTA, in part, amended Section 230 to weaken the statutory protection provided by Section 230(c)(1) to platforms that host user-generated content in an effort to combat sex trafficking. *See § 4, Pub. L. 115-164 (2018)*; 47 U.S.C. § 230(e)(5).

As a result, many platforms that hosted user-generated "adult" content immediately sought to mitigate their legal exposure under the new law to the detriment of Internet users. Although FOSTA was ostensibly intended

---

4. *See* Lenny Zeltser, *How antivirus software works; Virus detection techniques*, SearchSecurity.com (Oct. 2011) ("The biggest downside of heuristics is it can inadvertently flag legitimate files as malicious."), https://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques.

5. *See* Jason Kelley and Aaron Mackey, *Don't Repeat FOSTA's Mistakes*, EFF (March 29, 2019), https://www.eff.org/deeplinks/2019/03/dont-repeat-fostas-mistakes.

to curb unlawful content and related behavior, its silencing effect went far beyond unlawful speech. Craigslist, the online classified ads site, for example, shut down its personals section, a loss to people who used the section for lawful purposes.[6] Pounced, a niche dating site, shut down entirely because of FOSTA.[7] Other platforms appeared to react to the passage of FOSTA: Tumblr, the blogging site, banned all adult content,[8] while Facebook created a new "sexual solicitation" policy.[9]

The Fourth Circuit predicted the fallout that would occur with any weakening of Section 230(c)(1)'s immunity against liability for platforms that host user-generated content: "Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted." *Zeran v. AOL*, 129 F.3d 327, 331 (4th Cir. 1997) .

In light of online platforms' response to FOSTA, it is more than likely that filtering tool providers will take

---

6. Craigslist, *About FOSTA*, https://www.craigslist.org/about/FOSTA.

7. Samantha Cole, *Furry Dating Site Shuts Down Because of FOSTA*, Vice (April 2, 2018), https://www.vice.com/en_us/article/8xk8m4/furry-dating-site-pounced-is-down-fosta-sesta.

8. Shannon Liao, *Tumblr will ban all adult content on December 17th*, The Verge (Dec. 3, 2018), https://www.theverge.com/2018/12/3/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode.

9. *See* Elliot Harmon, *Facebook's Sexual Solicitation Policy is a Honeypot for Trolls*, EFF (Dec. 7, 2018), https://www.eff.org/deeplinks/2018/12/facebooks-sexual-solicitation-policy-honeypot-trolls.

similar steps to limit their legal exposure should the *Enigma* panel decision stand. But instead of taking down more user-generated content as platforms did in response to FOSTA, filtering tool providers will be reluctant to block certain software or content, as those decisions may later be alleged to have been the result of "anticompetitive animus" or "bad faith." This will dampen the market for innovative filtering technologies and may ultimately make users less safe online.

### D. An Unqualified Section 230(c)(2)(B) Immunity Ensures a Highly Competitive Market for Online Filtering Tools, Consistent with Congress' Goals

On the other hand, interpreting Section 230(c)(2)(B) as the plain language makes clear—that is, as creating an unqualified immunity for filtering tool providers—ensures a highly competitive market for such tools. With guaranteed immunity, many players will feel free to enter the filtering tool market, and filtering tool providers will feel free to engineer powerful products to the benefit of Internet users. Further, because these tools can produce false positives, broadly interpreting Section 230(c)(2)(B) ensures that filtering tool providers have the legal breathing room to make mistakes while striving to build better tools. This ultimately ensures that Internet users have a plethora of choices when looking for filtering tools, either for themselves or their families, workplaces, schools, libraries, and so on; it also ensures that platforms have choices so they can create online spaces for a diverse array of audiences.

The Ninth Circuit was correct that "Congress wanted to encourage the development of filtration technologies." *Enigma Software Group USA, LLC*, 946 F.3d at 1051. Unequivocal protection for filtering tool providers under Section 230(c)(2)(B) creates the market incentives consistent with Congress' stated policy goals:

> 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;" and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.

*See* 47 U.S.C. § 230(b)(3) & (b)(4). *See also Enigma Software Group USA, LLC*, 946 F.3d at 1055 (Rawlinson, J., dissenting) ("The majority's policy arguments are in conflict with our recognition in [*Zango Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009) ] that the broad language of the Act is consistent with 'the Congressional goals for immunity' as expressed in the language of the statute.").

## III. An Unqualified Section 230(c)(2)(B) Immunity Incentivizes Non-Profits Like EFF to Create Robust User-Empowerment Tools

The market incentives created by an unqualified Section 230(c)(2)(B) immunity do not apply just to for-profit companies. Non-profit, public interest organizations

also benefit from a broad reading of the law, including *amicus* EFF and the partners it works with. This is evidenced by two examples.

First, EFF's team of public interest technologists has developed a free privacy-enhancing tool called Privacy Badger,[10] which is a browser add-on that was designed for Internet users who want to browse the Internet without having a third party secretly track them.[11] Privacy Badger does not use a prespecified block list, but instead uses a heuristic to block content from domains that appear to be tracking Internet users.[12]

In some cases, this can lead to preventing Internet users from seeing ads from companies that track them—potentially including ads run by entities opposed to EFF's advocacy or the views EFF espouses, or even ads run by entities providing competing privacy-enhancing software (essentially the closest thing EFF has to "competitors").[13] Thus, EFF has created a kind of filtering tool and directly benefits from the immunity provided by Section 230(c)(2)(B). Should EFF face lawsuits alleging that it has somehow acted in "bad faith" by blocking third-party trackers and the ads they serve online, EFF's ability to continue providing free privacy-enhancing tools to Internet users will be seriously threatened.

---

10. *See generally Privacy Badger*, EFF, https://www.eff.org/privacybadger.

11. *What is Privacy Badger?*, EFF, https://www.eff.org/privacybadger/faq#What-is-Privacy-Badger.

12. *How does Privacy Badger work?*, EFF, https://www.eff.org/privacybadger/faq#How-does-Privacy-Badger-work.

13. *Why does Privacy Badger block ads?*, EFF, https://www.eff.org/privacybadger/faq#Why-does-Privacy-Badger-block-ads.

Second, EFF's Threat Lab team of cybersecurity researchers has recently been focusing on the problem of "spouseware" or "stalkerware," which is tracking software surreptitiously installed on someone's smartphone typically by a suspicious, paranoid, obsessed, or vindictive romantic partner.[14] These secret voyeurs are also often domestic violence perpetrators—and they use these tracking tools to terrorize their victims. Their victims often do not understand "[h]ow their abusers seem to know where they've been and sometimes even turn up at those locations to menace them," or "[h]ow they flaunt photos mysteriously obtained from the victim's phone, sometimes using them for harassment or blackmail."[15] EFF has been working to convince filtering tool companies to flag this kind of spyware, which is often marketed by the companies that develop it as legitimate.[16]

Kaspersky Lab—the defendant in the *Zango* case—heeded EFF's call and "added a feature to its Android antivirus app that alerts users if their data is being

---

14. Rebecca Jeschke, *EFF's New "Threat Lab" Dives Deep into Surveillance Technologies—And Their Use and Abuse*, EFF (April 4, 2019), https://www.eff.org/deeplinks/2019/04/effs-new-threat-lab-dives-deep-surveillance-technologies-and-their-use-and-abuse.

15. Andy Greenberg, *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*, Wired (April 3, 2019), https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/.

16. *See, e.g.*, Lisa Weintraub Schifferle, *Stalking apps: Retina-X settles charges*, Federal Trade Commission (Oct. 22, 2019) (describing an FTC settlement with a stalkerware app developer that created tools that "were marketed for monitoring children and employees, but in the wrong hands, they let abusers track people's physical movements and online activities"), https://www.consumer.ftc.gov/blog/2019/10/stalking-apps-retina-x-settles-charges/.

tracked by known spyware."[17] Given that one of EFF's goals is to eradicate stalkerware entirely, EFF fears that providers of filtering tools will no longer cooperate with EFF's requests to block stalkerware if doing so would expose them to potential lawsuits alleging that they have somehow acted in "bad faith" by blocking these spyware products, especially if stalkerware companies claim these products are actually legitimate.

## CONCLUSION

For the foregoing reasons, *amicus* requests that the Court grant Petitioner's writ of certiorari.

May 20, 2020

Respectfully submitted,

Sophia Cope
*Counsel of Record*
Aaron Mackey
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

*Attorneys for Amicus Curiae*

17. Sean Lyngaas, *Kaspersky Lab looks to combat "stalkerware" with new Android feature*, CyberScoop (April 3, 2019), https://www.cyberscoop.com/kaspersky-lab-looks-combat-stalkerware-new-android-feature/.