No. 19A___

IN THE

Supreme Court of the United States

MALWAREBYTES, INC.,

Applicant,

v.

ENIGMA SOFTWARE GROUP USA, LLC,

Respondent.

APPLICATION FOR AN EXTENSION OF TIME TO FILE A PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

NEAL KUMAR KATYAL
Counsel of Record
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600
neal.katyal@hoganlovells.com

March 6, 2020

Counsel for Applicant

APPLICATION

To the Honorable Elena Kagan, Associate Justice of the Supreme Court of the United States and Circuit Justice for the Ninth Circuit:

Pursuant to Rule 13.5 of the Rules of this Court and 28 U.S.C. § 2101(c), applicant Malwarebytes, Inc. respectfully requests a 40-day extension of time, to and including May 11, 2020,[1] within which to file a petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case. Applicant has consulted respondent's counsel, who has indicated that Respondent consents to this request.

1. The United States District Court for the Northern District of California entered its opinion dismissing the complaint against Malwarebytes on November 7, 2017 (Appendix A). The United States Court of Appeals for the Ninth Circuit issued its opinion in this case on September 12, 2019, 938 F.3d 1026 (Appendix B). Malwarebytes sought rehearing, which the court denied after modifying its opinion on December 31, 2019, 946 F.3d 1040 (Appendix C). Unless extended, the time to file a petition for certiorari in this Court will expire on March 30, 2020. This application is being filed more than ten days before the petition is currently due. *See* Sup. Ct. R. 13.5. The jurisdiction of this Court will be invoked under 28 U.S.C. § 1254(1).

2. In Section 230 of the Communications Decency Act (CDA), Congress enacted a system of self-regulation for the Internet by immunizing providers of fil-

[1] The fortieth day falls on Saturday, May 9, meaning the due date would be the following Monday in accordance with Rule 30.1.

tering technology from lawsuits, thereby encouraging the development of tools that would allow users to control the content they are exposed to. 47 U.S.C. § 230(c)(2). In the divided panel opinion below, the Ninth Circuit fashioned an exception to that immunity without identifying any basis for that exception in the text of the statute. *See* App'x C 18. Its approach to Section 230 differs from that of several other courts, including those of California.

3. Malwarebytes is a security company that develops software empowering users to protect themselves from the vast array of threats on the Internet. *See* App'x C 11. Employing its experience and judgment, in October 2016, Malwarebytes began classifying certain products of plaintiff Enigma Software Group as Potentially Unwanted Programs ("PUPs")—that is, programs that try to deceive users into thinking something is wrong with their computer to induce them to purchase a paid version of the PUP. *Id.* at 11-12. As with any PUP, Malwarebytes' software notified users of the potential risk and gave them a choice whether to continue using the Enigma product. *Id.*

4. Enigma sued Malwarebytes, alleging various business torts and unfair advertising in violation of the Lanham Act. Malwarebytes moved to dismiss, invoking the CDA's immunity from suit for any "provider or user of an interactive computer service" that takes "*any* action to enable or make available * * * the technical means to restrict access to" "material that the *provider* or user *considers to be* obscene, * * * harassing, or *otherwise objectionable*." 47 U.S.C. § 230(c)(2) (emphases added). Enigma opposed the motion. According to Enigma, Malwarebytes' true mo-

tivation was to stop consumers from using Enigma's products, which allegedly competed directly with Malwarebytes. *See* App'x C 12-13. Enigma urged the court to reject immunity under such circumstances.

5. The District Court granted Malwarebytes' motion to dismiss. App'x A 7. The court recognized that there was no motive-based exception to immunity for providers of filtering technology in the text of Section 230. *See id.* at 5. That omission is particularly telling given that the adjacent provision, which concerns entities that block content directly rather than leaving the choice to users, *does* contain a "good faith" requirement for immunity. *Id.* (comparing 47 U.S.C. § 230(c)(2)(A) with § 230(c)(2)(B)). Thus, the court "assume[d] that Congress acted intentionally when it decided to include a good-faith requirement in subsection (A) but not in (B)." *Id.* (citing *Connecticut National Bank* v. *Germain*, 503 U.S. 249, 253-254 (1992)). The court therefore rejected Enigma's contention that Section 230(c)(2)(B)'s immunity contains an unstated exception for supposedly "anticompetitive" conduct. *See id.* at 5-6.

6. In a divided decision, the Ninth Circuit reversed. *See* App'x C 25-27. The majority held that the "CDA's history and purpose" implied an exception to the statute's immunity when a plaintiff alleges that a provider has acted with "anticompetitive motives." *Id.* at 18. The panel acknowledged that the statute's text involved a "broad grant" of immunity but expressed concern that this text no longer adequately served "the statute's express policies," codified in subsections (a) and (b) of the Act. *Id.* at 19. That led the court to conclude "that if a provider's basis for ob-

jecting to and seeking to block materials is because those materials benefit a competitor, the objection would not" be covered by the statutory immunity. *Id.* at 21.[2]

7. Judge Rawlinson dissented. She emphasized that there was no basis in the "broadly worded Communications Decency Act" for the majority's newly-fashioned exception. *Id.* at 26 (internal quotation marks omitted). "The majority's real complaint," she continued, "is not that the district court construed the statute too broadly, but that the statute is written too broadly." *Id.* Such a defect "is one beyond [the court's] authority to correct." *Id.*

8. Malwarebytes sought rehearing. In response, the panel withdrew its original opinion and replaced a sentence suggesting a suit may be brought anytime a filtration decision rests on the identity of the speaker—not just when the decision had an allegedly anticompetitive motive. *Compare* App'x B 10, *with* App'x C 11. The panel otherwise made no changes to its result or reasoning, and the en banc court declined to rehear the case. *See* App'x C 4-5. Judge Rawlinson again dissented and indicated that she would have granted rehearing en banc. *Id.* at 4, 26-27.

9. The decision below defies elementary principles of statutory interpretation long articulated by this Court. The Ninth Circuit divined an exception to Section 230's immunity by relying exclusively on its views of the relevant policy considerations, unmoored from the text Congress enacted. *Id.* at 18-19. This Court's precedents forbid that approach. *See e.g.*, *Central Bank of Denver, N.A.* v.

[2] The Ninth Circuit also held that Enigma's false-advertising claims do not fall within the CDA's exception to immunity for "intellectual property" claims. App'x C 22-25. Malwarebytes does not plan to seek review of that issue.

First Interstate Bank of Denver, N.A., 511 U.S. 164, 188 (1994) ("[p]olicy considerations cannot * * * override interpretation of the text and structure of [an] Act"). The Ninth Circuit's treatment of Section 230 also breaks with several other courts, including those of California, the largest State in that circuit. *See, e.g.*, *Pallorium, Inc. v. Jared*, No. G036124, 2007 WL 80955, at *7 (Cal Ct. App. Jan. 11, 2007); *Prager Univ.* v. *Google, LLC*, No. 19-CV-340667, slip op. at 4 (Cal. Sup. Ct. Santa Clara Cty. Nov. 19, 2019), *appeal docketed* No. H047714 (Cal. Ct. App. 6th Dist. Dec. 19, 2019). The result threatens to replace the system of self-regulation that Congress enacted with judicial micromanagement of the Internet. This Court's review is warranted to bring the Ninth Circuit back into line on this important federal question.

10. Malwarebytes has retained Neal Kumar Katyal of Hogan Lovells US LLP as counsel to file a petition for writ of certiorari. Over the next several weeks, counsel is occupied with briefing deadlines and argument for a variety of matters, including: (a) a brief in opposition to certiorari in *K.G.S.* v. *Facebook, Inc.*, No. 19-910 (U.S.), due March 23; (b) a reply brief in support of certiorari in *Credit Bureau Center, LLC* v. *Federal Trade Commission*, No. 19-914 (U.S.), due April 6; (c) a reply brief on the merits in *Ford* v. *Bandemer*, No. 19-369 (U.S.) and *Ford* v. *Montana Eighth Judicial District*, No. 19-368 (U.S.), due approximately April 17, with argument to follow on April 27; and (d) a reply brief in support of certiorari in *Waggy* v. *United States*, No. 19-7544, due April 22. Applicant requests this extension of time to permit counsel to research the relevant legal and factual issues and to prepare a

petition that fully addresses the important questions raised by the proceedings below.

For these reasons, Applicant respectfully requests that an order be entered extending the time to file a petition for certiorari to and including May 11, 2020.

Respectfully submitted,

Neal Katyal / HB

NEAL KUMAR KATYAL
Counsel of Record
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600
neal.katyal@hoganlovells.com

March 6, 2020

Counsel for Applicant