

No. 19-

---

---

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**

---

**PETITION FOR A WRIT OF CERTIORARI**

---

TYLER GRIFFIN NEWBY  
FENWICK & WEST LLP  
555 California Street  
12th Floor  
San Francisco, CA 94104

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

*Counsel for Petitioner*

---

---

## QUESTION PRESENTED

Section 230(c)(2)(B) of the Communications Decency Act provides immunity from most civil liability to computer-service providers for “any action taken to enable or make available to \* \* \* others the technical means to restrict access to material” that “the provider or user considers to be \* \* \* objectionable.” 47 U.S.C. § 230(c)(2). The court below agreed that none of the narrow, express exceptions to that immunity in Section 230(e) apply here. The question presented is:

Whether federal courts can derive an implied exception to Section 230(c)(2)(B) immunity for blocking or filtering decisions when they are alleged to be “driven by anticompetitive animus.”

**PARTIES TO THE PROCEEDING**

Malwarebytes, Inc., petitioner on review, was the defendant-appellee below.

Enigma Software Group USA, LLC, respondent on review, was the plaintiff-appellant below.

**RULE 29.6 DISCLOSURE STATEMENT**

Malwarebytes, Inc. has no parent corporation, and no publicly held company owns 10% or more of its stock.

**RELATED PROCEEDINGS**

U.S. Court of Appeals for the Ninth Circuit:

*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, No. 17-17351 (9th Cir. Dec. 31, 2019) (reported at 946 F.3d 1040)

*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, No. 17-17351 (9th Cir. Sep. 12, 2019) (reported at 938 F.3d 1026) (opinion withdrawn and superseded on denial of rehearing)

U.S. District Court for the Northern District of California:

*Enigma Software Group USA LLC v. Malwarebytes Inc.*, No. 5:17-cv-02915-EJD (N.D. Cal. Nov. 7, 2017) (unreported)

## TABLE OF CONTENTS

	<u>Page</u>
QUESTION PRESENTED.....	i
PARTIES TO THE PROCEEDING.....	ii
RULE 29.6 DISCLOSURE STATEMENT .....	iii
RELATED PROCEEDINGS .....	iv
TABLE OF AUTHORITIES.....	vii
OPINIONS BELOW .....	1
JURISDICTION .....	1
STATUTORY PROVISIONS INVOLVED .....	2
INTRODUCTION.....	2
STATEMENT .....	5
A. Statutory Background.....	5
B. Procedural Background.....	7
REASONS FOR GRANTING THE PETITION .....	10
I. THE DECISION BELOW DEFIES THIS COURT’S BASIC RULES OF STATUTORY INTERPRETATION AND DEVIATES FROM COURTS’ SETTLED UNDERSTANDINGS OF SECTION 230 .....	10
A. The Decision Below Erroneously Relied On Policy Rather Than Text To Interpret Section 230 .....	11
B. The Decision Below Splits From The Approach Of Numerous Oth- er Courts .....	17
II. THE QUESTION PRESENTED IS OF SUBSTANTIAL IMPORTANCE.....	20

**TABLE OF CONTENTS—Continued**

	<u>Page</u>
A. The Decision Below Threatens The User Choice And Internet Security Goals That Motivated Section 230(c)(2)(B) .....	21
B. The Decision Below Will Under- mine Other Tools That Help In- ternet Users Curate Their Own Online Experience .....	29
C. The Decision Below Endangers All Of Section 230’s Important Immunities .....	31
III. THIS CASE IS AN IDEAL VEHICLE TO RESOLVE THE QUESTION PRESENTED, AND OTHER OPPORTUNITIES MAY NOT SOON PRESENT THEMSELVES .....	35
CONCLUSION .....	37
APPENDIX	
APPENDIX A—Ninth Circuit’s Amend- ed Opinion (Dec. 31, 2019) .....	1a
APPENDIX B—Ninth Circuit’s Opinion (Sept. 12, 2019) .....	30a
APPENDIX C—District Court’s Order Granting Defendant’s Motion to Dismiss (Nov. 7, 2017) .....	57a
APPENDIX D—Statutory Provisions Involved .....	66a

**TABLE OF AUTHORITIES**

	<u>Page(s)</u>
<b>CASES:</b>	
<i>Almeida v. Amazon.com, Inc.</i> , 456 F.3d 1316 (11th Cir. 2006).....	18
<i>Barnhart v. Sigmon Coal Co.</i> , 534 U.S. 438 (2002).....	11, 12
<i>Barrett v. Rosenthal</i> , 146 P.3d 510 (Cal. 2006).....	20
<i>BP Am. Prod. Co. v. Burton</i> , 549 U.S. 84 (2006).....	11
<i>Cent. Bank of Denver, N.A., v. First Inter- state Bank of Denver, N.A.</i> , 511 U.S. 164 (1994).....	12
<i>Chicago Lawyers’ Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.</i> , 519 F.3d 666 (7th Cir. 2008).....	17
<i>Comcast Corp. v. Federal Communications Commission</i> , 600 F.3d 642 (D.C. Cir. 2010).....	19
<i>Diamond v. Chakrabarty</i> , 447 U.S. 303 (1980).....	12
<i>Doe v. GTE Corp.</i> , 347 F.3d 655 (7th Cir. 2003).....	31, 32
<i>Doe v. Internet Brands, Inc.</i> , 824 F.3d 846 (9th Cir. 2016).....	18
<i>Doe v. MySpace, Inc.</i> , 528 F.3d 413 (5th Cir. 2008).....	18



**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
<i>Dunn v. Commodity Futures Trading Comm’n, 519 U.S. 465 (1997)</i> .....	12
<i>Eastman Kodak Co. v. Image Tech. Servs., Inc., 504 U.S. 451 (1992)</i> .....	28
<i>Fair Hous. Council of San Fernando Val- ley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008)</i> .....	25
<i>Fed. Mar. Comm’n v. S.C. State Ports Auth., 535 U.S. 743 (2002)</i> .....	24
<i>Fehrenbach v. Zeldin, No. 17-CV-5282 (JFB) (ARL), 2018 WL 4242452 (E.D.N.Y. Aug. 6, 2018), report and recommendation adopted, 2018 WL 4242453 (E.D.N.Y. Sept. 5, 2018)</i> .....	29
<i>Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356 (2019)</i> .....	5, 10, 12
<i>Force v. Facebook, 934 F.3d 53 (2d Cir. 2019), petition for cert. filed, No. 19-859 (U.S. Jan. 2, 2020)</i> .....	17
<i>Hassell v. Bird, 420 P.3d 776 (Cal. 2018)</i> .....	17
<i>Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016)</i> .....	17, 23

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
<i>Johnson v. Arden</i> , 614 F.3d 785 (8th Cir. 2010).....	18
<i>Marshall’s Locksmith Serv. Inc. v. Google, LLC</i> , 925 F.3d 1263 (D.C. Cir. 2019).....	18
<i>Michigan v. Bay Mills Indian Cmty.</i> , 572 U.S. 782 (2014).....	14
<i>Mitchell v. Forsyth</i> , 472 U.S. 511 (1985).....	25
<i>Nat’l Org. for Women, Inc. v. Scheidler</i> , 510 U.S. 249 (1994).....	14
<i>Nemet Chevrolet, Ltd. v. Consumeraf-fairs.com, Inc.</i> , 591 F.3d 250 (4th Cir. 2009).....	24
<i>N.Y. State Conference of Blue Cross &amp; Blue Shield Plans v. Travelers Ins. Co.</i> , 514 U.S. 645 (1995).....	12
<i>Pallorium, Inc. v. Jared</i> , No. G036124, 2007 WL 80955 (Cal. Ct. App. Jan. 11, 2007) .....	20
<i>Perry v. Perez</i> , 565 U.S. 388 (2012).....	15
<i>Prager Univ. v. Google LLC</i> , No. 19CV340667, 2019 WL 8640569 (Cal. Super. Ct. Nov. 19, 2019), <i>appeal docketed</i> , No. H047714 (Cal. Ct. App. Dec. 19, 2019).....	19, 20

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	23
<i>Romag Fasteners, Inc. v. Fossil Grp., Inc.</i> , __ S. Ct. __ (2020).....	14
<i>Russello v. United States</i> , 464 U.S. 16 (1983).....	13
<i>Sebelius v. Cloer</i> , 569 U.S. 369 (2013).....	11
<i>Shiamili v. Real Estate Grp. of N.Y., Inc.</i> , 952 N.E.2d 1011 (N.Y. 2011).....	17, 18
<i>Stratton Oakmont, Inc. v. Prodigy Servs.</i> <i>Co.</i> , No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995).....	6, 23
<i>Wisconsin Cent. Ltd. v. United States</i> , 138 S. Ct. 2067 (2018).....	13, 16
<i>Yates v. United States</i> , 574 U.S. 528 (2015).....	16
<i>Zango, Inc. v. Kaspersky Lab, Inc.</i> , 568 F.3d 1169 (9th Cir. 2009).....	7, 10, 25
<i>Zeran v. Am. Online, Inc.</i> , 129 F.3d 327 (4th Cir. 1997).....	<i>passim</i>
<b>STATUTES:</b>	
28 U.S.C. § 1254(1) .....	2
Communications Decency Act.....	<i>passim</i>
47 U.S.C. § 230.....	<i>passim</i>

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
47 U.S.C. § 230(a) .....	34
47 U.S.C. § 230(a)(1) .....	34
47 U.S.C. § 230(a)(2) .....	22
47 U.S.C. § 230(a)(3) .....	34
47 U.S.C. § 230(a)(4) .....	22
47 U.S.C. § 230(b) .....	18, 34
47 U.S.C. § 230(b)(1) .....	34
47 U.S.C. § 230(b)(2)-(4).....	22
47 U.S.C. § 230(b)(2) .....	24, 28
47 U.S.C. § 230(b)(3) .....	5, 19, 30
47 U.S.C. § 230(b)(4) .....	5, 19
47 U.S.C. § 230(c).....	<i>passim</i>
47 U.S.C. § 230(c)(1) .....	<i>passim</i>
47 U.S.C. § 230(c)(2) .....	<i>passim</i>
47 U.S.C. § 230(c)(2)(A).....	<i>passim</i>
47 U.S.C. § 230(c)(2)(B).....	<i>passim</i>
47 U.S.C. § 230(c)-(e) .....	18
47 U.S.C. § 230(e).....	7
47 U.S.C. § 230(e)(2) .....	7
47 U.S.C. § 230(e)(4) .....	7
<b>RULE:</b>	
Sup. Ct. R. 10(c).....	16
<b>LEGISLATIVE MATERIAL:</b>	
141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox) .....	5, 22
H.R. Conf. Rep. No. 104-458 (1996), <i>as reprinted in</i> 1996 U.S.C.C.A.N. 10 .....	23

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
<b>OTHER AUTHORITIES:</b>	
<i>About Direct Messages</i> , Twitter, <a href="https://bit.ly/3bldCQ2">https://bit.ly/3bldCQ2</a> (last visited May 11, 2020) .....	30
<i>About the Notifications timeline</i> , Twitter, <a href="https://bit.ly/3eu7VRv">https://bit.ly/3eu7VRv</a> (last visited May 11, 2020) .....	30
The American Heritage College Dictionary (3d ed. 1993) .....	16
<i>Community Standards: Part III. Objec- tionable Content</i> , Facebook, <a href="https://bit.ly/2KgiUAq">https://bit.ly/2KgiUAq</a> (last visited May 11, 2020) .....	33
Eric Goldman, <i>The Ten Most Important Section 230 Rulings</i> , 20 <i>Tulane J. Tech. &amp; Intell. Prop.</i> 1 (2017) .....	36
Eric Griffith, <i>How to Rid a New PC of Crapware</i> , <i>PCMag</i> (Apr. 1, 2020), <a href="https://bit.ly/3ch9BMM">https://bit.ly/3ch9BMM</a> .....	26
Kate Klonick, <i>The New Governors: The People, Rules, and Processes Governing Online Speech</i> , 131 <i>Harv. L. Rev.</i> 1598 (2018) .....	32
Jeff Kosseff, <i>The Twenty-Six Words That Created the Internet</i> (2019) .....	33

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
Mike Masnick, <i>Masnick’s Impossibility Theorem: Content Moderation At Scale Is Impossible To Do Well</i> , TechDirt (Nov. 20, 2019), <a href="https://bit.ly/2z1XpRh">https://bit.ly/2z1XpRh</a> .....	32
Press Release, FTC, <i>FTC Case Results in \$163 Million Judgment Against “Scareware” Marketer</i> (Oct. 2, 2012), <a href="https://bit.ly/3bjkJIx">https://bit.ly/3bjkJIx</a> .....	26
Press Release, FTC, <i>Office Depot and Tech Support Firm Will Pay \$35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services</i> (Mar. 27, 2019), <a href="https://bit.ly/3afWpWH">https://bit.ly/3afWpWH</a> .....	26
Press Release, Senator Ted Cruz, <i>Sen. Cruz: The Pattern of Political Censorship Seen Across Technology Companies is Highly Concerning</i> (Jan. 17, 2018), <a href="https://bit.ly/2zdfuMB">https://bit.ly/2zdfuMB</a> .....	34
Senator Josh Hawley (@HawleyMO), Twitter (Nov. 27, 2018, 1:22 PM), <a href="https://bit.ly/2VB3CLQ">https://bit.ly/2VB3CLQ</a> .....	34
<i>Transparency Report 2019</i> , Reddit, <a href="https://bit.ly/2ysFhj9">https://bit.ly/2ysFhj9</a> (last visited May 11, 2020) .....	30
Webster’s II New College Dictionary (1995 ed.) .....	16

**TABLE OF AUTHORITIES—Continued**

	<u>Page(s)</u>
YouTube Help, <i>Disable or enable Restricted Mode</i> , Google, <a href="https://bit.ly/2KftqaQ">https://bit.ly/2KftqaQ</a> (last visited May 11, 2020) .....	29

IN THE  
**Supreme Court of the United States**

---

No. 19-

---

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**

---

**PETITION FOR A WRIT OF CERTIORARI**

---

Malwarebytes, Inc., respectfully petitions for a writ of certiorari to review the judgment of the Ninth Circuit in this case.

**OPINIONS BELOW**

The Ninth Circuit's amended opinion, issued on denial of rehearing, is reported at 946 F.3d 1040. Pet. App. 1a-29a. Its original, superseded opinion is reported at 938 F.3d 1026. Pet. App. 30a-56a. The district court's order granting Malwarebytes's motion to dismiss is unreported. *Id.* at 57a-65a.

**JURISDICTION**

The Ninth Circuit entered judgment on September 12, 2019. Pet. App. 1a, 30a. Malwarebytes timely



petitioned for panel rehearing and rehearing en banc, which were denied on December 31, 2019. *Id.* at 1a, 4a-5a. Justice Kagan extended the time to file a petition for certiorari to May 11, 2020. This Court’s jurisdiction rests on 28 U.S.C. § 1254(1).

### **STATUTORY PROVISIONS INVOLVED**

Section 230(c)(2) of the Communications Decency Act, 47 U.S.C. § 230(c)(2), provides that:

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

The entirety of Section 230 is reproduced in the appendix to this petition, Pet. App. 66a-71a, as is the text of Section 230 as it appeared before its 2018 amendments, *id.* at 72a-76a.

### **INTRODUCTION**

The Communications Decency Act (CDA) is foundational to the Internet as we know it. Faced with a revolutionary new technology, Congress chose a system of self-regulation—one that would leave users, rather than governments or courts, in control

of their own experience. The cornerstone of that system is the immunity from civil liability provided in Section 230(c). Through that provision, Congress ensured that Internet providers and users would be free from the constant threat of litigation for moderating threatening or objectionable content. Of course, that would be impossible without adequate tools for screening and filtering content. Thus, in Section 230(c)(2)(B), Congress extended that immunity—without qualification—to providers for “any action taken to enable or make available” the “technical means to restrict access to” content the provider “considers to be” objectionable. 47 U.S.C. § 230(c)(2).

Petitioner Malwarebytes, Inc., is a leading software security firm that provides filtering tools to consumers. Its software flags security threats and other unwanted programs, and asks users whether they wish to retain those programs. After an update to Malwarebytes’s software began flagging Respondent’s products as potentially unwanted programs and providing its users the choice to use or to quarantine the products, Respondent sued Malwarebytes. The plain text of the Act forbids exactly this kind of retaliatory suit.

In the decision below, however, a divided panel of the Ninth Circuit read the Act to contain an implied exception for actions allegedly motivated by “anti-competitive animus.” To its credit, the court did not even try to justify that reading based on the text of the statute. Instead, the court relied exclusively on its own mistaken understanding of the policy interests at stake.

This Court's precedents flatly forbid that approach. In recent decades, this Court has instructed lower courts that statutory interpretation must be guided, first and foremost, by the text, and that even compelling policy considerations cannot justify an interpretation that runs counter to the text. The decision below defies that cardinal rule. It is therefore no surprise that—in both its reasoning and holding—the decision breaks from decisions of numerous other courts. And the conflict has only gotten worse in the short time since the court issued its decision, as a California state court has already issued a decision expressly disagreeing with it—opening a rift between state and federal fora in the technology center of the Nation.

It is critically important for the Court to correct the Ninth Circuit's erroneous interpretation now. By exposing developers of filtering tools to a flood of retaliatory litigation, the decision will have the opposite effect from Congress's goal of promoting development of such tools. Making matters worse, because the Ninth Circuit relied solely on policy considerations that apply to all of Section 230, its decision threatens *all* of Section 230(c)'s immunities. It is an open invitation for lower courts to allow a lawsuit anytime judges have their own policy concerns about a particular filtering decision or tool. The decision below thus risks exposing cybersecurity firms, as well as the most popular Internet services, to a raft of burdensome litigation for providing the filtering tools and exercising the content-moderation and editorial discretion that Congress sought to encourage. The result will be an Internet with less

consumer choice and less protection for users from offensive and objectionable content.

The decision below is a throwback to “a bygone era of statutory construction,” when judges looked primarily to ill-defined indicia of congressional intent rather than statutory text. *Food Mktg. Inst. v. Argus Leader Media*, 139 S. Ct. 2356, 2364 (2019) (internal quotation marks omitted). The Court should grant certiorari to correct the Ninth Circuit’s “casual disregard of the rules of statutory interpretation” and bring it back in line with the prevailing interpretations of Section 230. *Id.*

The petition should be granted.

## STATEMENT

### A. Statutory Background

The CDA emerged in 1996 as a response to the proliferation of offensive content on the nascent Internet. Congress sought an innovative approach for this new technology, one that would let “Government \* \* \* get out of the way and let parents and individuals” “tailor what [they] see to [their] own tastes.” 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox). The resulting Act therefore aimed “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 “to remove disincentives for the development and utilization of blocking and filtering technologies.” 47 U.S.C. § 230(b)(3), (4).

Congress identified the threat of litigation as a particular obstacle to the development of “blocking and filtering technologies.” *See* Pet. App. 8a-10a.

Early state-court decisions had made it challenging for Internet-based firms to take action against offensive or dangerous content by exposing those who did to liability. *See id.* (discussing *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995)).

The operative text of the CDA took a three-pronged approach to eliminating the threat of such litigation.

First, in subsection (c)(1), Congress addressed immunity for hosting third-party content. It ensured that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1). That provision bars suits seeking to hold providers liable for exercising “a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content.” *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

Second, in subsection (c)(2)(A), Congress provided immunity for those who block or filter content. Specifically, it barred civil liability against “provider[s]” and “user[s] of an interactive computer service” who take action “to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” 47 U.S.C. § 230(c)(2)(A). That immunity is available for “any action,” so long as it is “voluntarily taken in good faith.” *Id.*

Third—and most relevant here—in subsection (c)(2)(B), Congress extended immunity to entities that develop and provide the technology necessary

for filtering and blocking content. That immunity covers “any action taken to enable or make available \* \* \* the technical means to restrict access to” the material described in subsection (c)(2)(A),<sup>1</sup> *id.* § 230(c)(2)(B)—that is, “material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable,” *id.* § 230(c)(2)(A). Unlike the immunity for those who themselves “*restrict* access to or availability of” such material, the immunity for developers of filtering technology is not conditioned on “good faith.” *Compare id.* (emphasis added), *with id.* § 230(c)(2)(B).

Congress also provided a handful of exceptions to the CDA’s immunity, including with respect to intellectual property laws and communications privacy laws. *See, e.g., id.* § 230(e)(2), (4). None of those exceptions refers to antitrust law or “anticompetitive” behavior. *See id.* § 230(e).

## **B. Procedural Background**

1. Malwarebytes is an Internet security firm with an international customer base. Pet. App. 12a. Users download its software to protect themselves from a wide array of threats on the Internet. These include “malware,” which can damage operating systems or steal user information, and “Potentially Unwanted Programs” (or “PUPs”) that falsely de-

---

<sup>1</sup> As enacted, the text cross-references subsection (c)(1), *see* 47 U.S.C. § 230(c)(2)(B), but that is uniformly regarded as a scrivener’s error, *see Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 n.5 (9th Cir. 2009).

ceive users into thinking something is wrong with their computer so that they will download paid products to combat the supposed threats. *See id.* When Malwarebytes’s “software detects an unwanted program, it displays a notification and asks the user if she wants to remove the program from her computer.” *Id.* at 58a. In other words, users make the final decision about what gets filtered.

In October 2016, Malwarebytes adopted new criteria for identifying a PUP. *Id.* at 12a-13a. Using those criteria, Malwarebytes’s software began classifying certain products of Respondent Enigma Software Group as a PUP. *Id.* As with any PUP, Malwarebytes’ software gave users the option to retain, quarantine, or remove Enigma’s products. *Id.* at 12a-13a, 58a.

2. Enigma sued Malwarebytes, alleging state-law business torts and unfair advertising in violation of the Lanham Act. *Id.* at 58a-59a. Malwarebytes moved to dismiss, invoking Section 230(c)(2)(B)’s immunity for providers of filtering software. *Id.* at 14a. Enigma opposed the motion, claiming “that Malwarebytes blocked Enigma’s programs for anti-competitive reasons” and that the CDA’s immunity is unavailable under such circumstances. *Id.* at 19a.

The District Court granted Malwarebytes’s motion. *Id.* at 65a. It held that “the plain language of the statute” requires only that “*the provider* or user consider[.]” the filtered material “objectionable.” *Id.* at 62a (quoting 47 U.S.C. § 230(c)(2)). Thus, it was irrelevant *why* Malwarebytes considered Enigma’s products “objectionable.” *See id.* The court noted that the neighboring provision addressing immunity

for those who actually “restrict access” to content “include[s] a good-faith requirement.” *See id.* at 63a (discussing 47 U.S.C. § 230(c)(2)(A)). Because Congress “chose not to” “include[] a similar reference” to good faith in subsection (c)(2)(B), the court declined to find a similar exception implied there. *Id.*

3. A divided panel of the Ninth Circuit reversed. *Id.* at 27a. Looking to the “history and purpose” of the CDA, *id.* at 19a, the majority held that Section 230(c)(2)’s immunity provisions contain an unstated exception for “decisions that are driven by anticompetitive animus,” *id.* at 11a. Although the court acknowledged that its reading was in tension with “the unwillingness of Congress to spell out the meaning of ‘otherwise objectionable,’” it felt obliged to update the statute for “today” by reading it not “to give providers unbridled discretion to block online content.” *Id.* at 20a. Although the court did not explain how its reading was compatible with the operative text of the statute or the ordinary meaning of the word “objectionable,” it found support for its reading in “the statute’s express policies.” *Id.* at 20a-21a.<sup>2</sup>

Judge Rawlinson dissented. The majority’s reading, she explained, “cannot be squared with the broad language of the Act.” *Id.* at 29a. “Under the language of the statute, if the blocked content is

---

<sup>2</sup> Separately, the court rejected Enigma’s argument that its Lanham Act false-advertising claim falls within the CDA’s exception for “intellectual property” law. Pet. App. 23a-27a. Malwarebytes does not seek review of this issue.



‘otherwise objectionable’ to the provider, the Act bestows immunity.” *Id.* (quoting *Zango*, 568 F.3d at 1173). “The majority’s real complaint,” the dissent pointed out, “is not that the district court construed the statute too broadly, but that the statute is written too broadly.” *Id.* at 28a. Such an issue “is one beyond [judicial] authority to correct.” *Id.*

Over Judge Rawlinson’s dissent, the Ninth Circuit denied Malwarebytes’s petition for rehearing and rehearing en banc. *Id.* at 4a-5a.<sup>3</sup> This timely petition followed.

## **REASONS FOR GRANTING THE PETITION**

### **I. THE DECISION BELOW DEFIES THIS COURT’S BASIC RULES OF STATUTORY INTERPRETATION AND DEVIATES FROM COURTS’ SETTLED UNDERSTANDINGS OF SECTION 230.**

One of this Court’s most fundamental precepts is that statutory interpretation must begin with the text—and end there when the text is clear. This Court has repeatedly granted certiorari to clarify that principle. *See, e.g., Food Mktg. Inst.*, 139 S. Ct. at 2364 (“We cannot approve such a casual disregard of the rules of statutory interpretation.”).

---

<sup>3</sup> The panel issued an amended opinion that modified a sentence suggesting that immunity would be unavailable *anytime* a decision was motivated by “the identity of the entity that produced” the filtered content. *Compare* Pet. App. 39a, *with id.* at 11a-12a. It made no other changes.

The Ninth Circuit flouted that rule in this case. The court never explained how its reading bears any relationship to the operative text of the statute. Instead, it relied exclusively on its own policy concerns (which were themselves questionable). Unsurprisingly, that fundamentally flawed approach led the court to the wrong outcome in this case.

Not only did the Ninth Circuit's approach defy this Court's precedent, it upended the widely-shared consensus among lower courts that Section 230's immunity provisions should be read broadly. The court also broke from the D.C. Circuit by using the CDA's prefatory statutory goals to override its operative text, and the resulting interpretation of subsection (c)(2)(B) has been flatly rejected by state courts in the very same State where this litigation arose, California. These conflicts on an issue of critical importance further counsel this Court's intervention.

**A. The Decision Below Erroneously Relied On Policy Rather Than Text To Interpret Section 230.**

1. “[I]n any statutory construction case,” a court must “start, of course, with the statutory text.” *Sebelius v. Cloer*, 569 U.S. 369, 376 (2013) (quoting *BP Am. Prod. Co. v. Burton*, 549 U.S. 84, 91 (2006)). This Court's cases insisting on that approach are legion. *See, e.g., Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 461-462 (2002) (“We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.”).

“When the words of a statute are unambiguous, then, this first canon is also the last: judicial inquiry is complete.” *Id.* at 462 (internal quotation marks omitted). A statute’s text is not “ambiguous” merely because it uses “[b]road general language.” *Diamond v. Chakrabarty*, 447 U.S. 303, 315 (1980). Only after examining “the text of the provision in question” and discerning a genuine ambiguity may a court “move on, as need be, to the structure and purpose of the Act in which it occurs.” *N.Y. State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 655 (1995); accord *Food Mktg. Inst.*, 139 S. Ct. at 2364 (finding it “inappropriate[ ]” to “resort to legislative history before consulting [a] statute’s text and structure”). Courts “[l]ack[ ] the expertise or authority to assess the[ ] important competing claims” involved in policy disputes, which are “best addressed to the Congress.” *Dunn v. Commodity Futures Trading Comm’n*, 519 U.S. 465, 480 (1997). And, critically, “[p]olicy considerations cannot override [an] interpretation of the text and structure of [an] Act.” *Cent. Bank of Denver, N.A., v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 188 (1994).

2. The Ninth Circuit broke sharply from this method of statutory interpretation. It started with its view of the statute’s “history and purpose,” not text. Pet. App. 19a. Indeed, the court apparently recognized that its approach was *incompatible* with Section 230’s text: It took note of Congress’s “unwillingness \* \* \* to spell out the meaning of ‘otherwise objectionable,’” and acknowledged that the text confers a “broad grant of protective control” to Internet providers. *Id.* at 20a.

Although the court linked its reading of the statute to the word “objectionable,” *id.* at 23a, that relationship was not based on the “ordinary \* \* \* meaning” of the term, as this Court’s cases require, *Wisconsin Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2074 (2018) (internal quotation marks omitted). The Ninth Circuit did not, for example, consider a definition of the term, or examine its meaning in other contexts. Instead, the court relied exclusively on two judges’ perspective of the underlying policy interests. Pet. App. 20a (expressing concern that “[u]sers would not reasonably anticipate providers blocking valuable online content”). In fact, the court properly *rejected* Enigma’s only argument based on the meaning of the word “objectionable.” *See id.* at 21a (refusing to apply *ejusdem generis* to narrow the meaning of “objectionable” given the “breadth of the term” and the lack of similarity among subsection (c)(2)’s “enumerated categories”).

By reading an unstated exception into the Act, the Ninth Circuit ignored a tried-and-true canon of textual analysis. “Where 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 quotation marks and alteration omitted). Here, Congress included a “good faith” requirement to claim immunity under subsection (c)(2)(A). The absence of any similar language indicates the “intentional[ ] \* \* \* exclusion” of any similar motive-based requirement for subsection (c)(2)(B)’s immunity.

Malwarebytes made this point in its appellate brief, Malwarebytes C.A. Answering Br. 29-30, and rehearing petition, C.A. Reh’g Pet. 11-12. Yet the panel majority failed to even acknowledge it.

The court’s sole justification for bypassing all of these bedrock rules of construction was policy. Pet. App. 19a-21a. Under this Court’s precedent, that is no justification at all. Courts have “no roving license, in even ordinary cases of statutory interpretation, to disregard clear language simply on the view that \* \* \* Congress ‘must have intended’ something” else. *Michigan v. Bay Mills Indian Cmty.*, 572 U.S. 782, 794 (2014); see also *Romag Fasteners, Inc. v. Fossil Grp., Inc.*, \_\_ S. Ct. \_\_, slip op. at 7 (2020) (“[T]he place for reconciling competing and incommensurable policy goals \* \* \* is before policymakers.”). The Ninth Circuit suggested that its emphasis on policy might be justified by Congress’s inclusion of policy statements in the CDA. See Pet. App. 11a, 20a-21a. Wrong again. Congressional findings are too “thin” a “reed upon which to base” an exception for “motive” that is “neither expressed nor \* \* \* fairly implied in the operative sections of the Act.” *Nat’l Org. for Women, Inc. v. Scheidler*, 510 U.S. 249, 260 (1994).

Making matters worse, the policy concern animating the majority was wholly unfounded. The panel feared that users would lose access to “valuable online content” because providers might “act for their own, and not the public, benefit.” Pet. App. 20a. But Congress anticipated this very issue. This case concerns immunity under subsection (c)(2)(B), which applies only to entities that empower *others* to filter

content by supplying the “technical means” to do so. 47 U.S.C. § 230(c)(2)(B). The majority’s concern is directed to those who “restrict access to or availability of material” under subsection (c)(2)(A), and that immunity is available only to those who act “in good faith.” *Id.* § 230(c)(2)(A).<sup>4</sup> The majority’s apparent confusion about this elementary issue only reinforces this Court’s longstanding position that courts are “ill suited” “to make \* \* \* policy judgments.” *Perry v. Perez*, 565 U.S. 388, 393 (2012) (per curiam); *see also infra* pp. 21-29 (explaining why Malwarebytes’s position better comports with Congress’s stated policies to promote competition and user choice).

3. The Ninth Circuit’s deeply flawed approach to statutory construction led it to an erroneous result. Under a plain-meaning analysis of Section 230’s “broad language,” Pet. App. 29a (Rawlinson, J., dissenting), Malwarebytes is entitled to immunity under subsection (c)(2)(B).

That provision immunizes (1) a “provider or user of an interactive computer service” that (2) offers to “others the technical means to restrict access to material” that (3) “the provider or user considers \* \* \* harassing[ ] or otherwise objectionable.” 47 U.S.C. § 230(c)(2). Only the third element was contested here, which makes sense: Malwarebytes’s software is plainly an interactive computer service,

---

<sup>4</sup> Because Malwarebytes only claims immunity under subsection (c)(2)(B), Malwarebytes takes no position on whether the conduct alleged by Enigma in this case would fall short of the “good faith” required by subsection (c)(2)(A).

and it operates by giving users the “technical means,” *id.* § 230(c)(2)(B), “to remove [a flagged] program from her computer,” Pet. App. 58a.

That leaves only whether Enigma’s products are “material that the provider” (here, Malwarebytes) “considers to be \* \* \* objectionable.” 47 U.S.C. § 230(c)(2)(A). Enigma’s complaint answers that question in the affirmative by conceding that Malwarebytes considers Enigma’s products “PUPs and ‘threats.’” C.A. E.R. 24. Because the Act requires only that Malwarebytes “considers” the content to be “objectionable,” that determination is sufficient for immunity to apply. The “ordinary, contemporary, common meaning,” *Wisconsin Cent.*, 138 S. Ct. at 2074 (internal quotation marks omitted), of “objectionable” is easily capacious enough to encompass programs that Malwarebytes has deemed a “threat” or a “potentially unwanted program.” *See, e.g.*, Webster’s II New College Dictionary (1995 ed.) (defining “objectionable” as “[p]rovoking disapproval or opposition: offensive”); The American Heritage College Dictionary (3d ed. 1993) (similar definition). Section 230(c)’s caption reinforces that reading. *See Yates v. United States*, 574 U.S. 528, 539-540 (2015) (plurality op.). It clarifies the provision is meant to protect “blocking and screening of *offensive* material,” even though the word “offensive” is not one of the enumerated categories in § 230(c)(2)’s list. 47 U.S.C. § 230(c) (emphasis added).

Because the Ninth Circuit only reached a contrary decision by disregarding this Court’s rules for statutory interpretation, this Court’s review is warranted. *See Sup. Ct. R.* 10(c). Allowing the decision below to

stand will embolden lower courts to carve out additional policy-driven exceptions to Congress's duly-enacted legislation. *See infra* pp. 31-35.

**B. The Decision Below Splits From The Approach Of Numerous Other Courts.**

Given how starkly the decision below deviates from this Court's precedents, it is no surprise that it renders the Ninth Circuit an outlier on Section 230 immunity.

1. Outside of the Ninth Circuit, courts are in agreement that Section 230's immunity provisions must be read expansively. As the Seventh Circuit has explained, that conclusion flows from Congress's choice to use broad language: "[T]he reason a legislature writes a general statute is to avoid any need to traipse through the United States Code" and state lawbooks to "consider all potential sources of liability, one at a time." *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008). Courts have widely honored that choice in the context of Section 230. *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18 (1st Cir. 2016) ("There has been near-universal agreement that section 230 should not be construed grudgingly."); *Force v. Facebook*, 934 F.3d 53, 64 (2d Cir. 2019) (noting "general agreement" that the CDA "should be construed broadly in favor of immunity"), *petition for cert. filed*, No. 19-859 (U.S. Jan. 2, 2020); *Zeran*, 129 F.3d at 331 (referring to "§ 230's broad immunity"); *Hassell v. Bird*, 420 P.3d 776, 788 (Cal. 2018) (plurality op.) ("the tools of statutory interpretation compel[ ] a broad construction of section 230"); *Shiamili v. Real Estate Grp. of N.Y., Inc.*, 952 N.E.2d



1011, 1016 (N.Y. 2011) (“Both state and federal courts around the country have generally interpreted Section 230 immunity broadly \* \* \* .” (internal quotation marks omitted)); *accord Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008); *Johnson v. Arden*, 614 F.3d 785, 791 (8th Cir. 2010); *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006); *Marshall’s Locksmith Serv. Inc. v. Google, LLC*, 925 F.3d 1263, 1267 (D.C. Cir. 2019).<sup>5</sup>

The decision below, however, takes the opposite approach. Motivated by policy concerns, it discerned “limitations in the scope of immunity” found nowhere in the Act’s text. Pet. App. 18a. The Ninth Circuit therefore eschewed the broad reading of Section 230 adopted by other courts. And this is not the first time that the Ninth Circuit has resorted to policy arguments to give the CDA a narrow construction. *See Doe v. Internet Brands, Inc.*, 824 F.3d 846, 851-853 (9th Cir. 2016) (reading the Act to have a “narrow language and \* \* \* purpose”). This decision cements the court’s outlier status.

2. The decision below also places the Ninth Circuit in square conflict with the D.C. Circuit regarding the proper relationship of Section 230’s express policy goals, *see* 47 U.S.C. § 230(b), with its operative text, *see id.* § 230(c)-(e). The panel repeatedly—and selectively—resorted to subsection (b)’s policy goals

---

<sup>5</sup> Although some of these decisions speak specifically in terms of subsection (c)(1), that merely reflects the facts of those cases. Nothing in the opinions’ reasoning suggests the broad reading is limited to that subsection.

to justify its atextual approach to statutory construction. See Pet. App. 20a-21a (citing 47 U.S.C. § 230(b)(3), (4)).

The D.C. Circuit has rejected that analytical approach. In *Comcast Corp. v. Federal Communications Commission*, 600 F.3d 642 (D.C. Cir. 2010), the FCC argued that it possessed regulatory power over “an Internet service provider’s network management practices.” *Id.* at 644. Lacking any “express statutory authority over such practices,” *id.*, the Commission turned to the policy goals enacted in subsection (b) of the CDA, claiming those goals could “anchor the exercise of [regulatory] authority” even without an express grant of power. *Id.* at 652. The D.C. Circuit rejected that argument, holding that “statements of policy, by themselves, do not create ‘statutorily mandated responsibilities.’” *Id.* at 644. The alternative approach, the court explained, would “virtually free the Commission from its congressional tether.” *Id.* at 655. The D.C. Circuit’s approach is flatly at odds with Enigma’s efforts to carve out an exception to the “statutorily mandated” immunity by relying on the CDA’s “policy statements alone.” *Id.* at 644, 654 (internal quotation marks omitted).

3. In near-record time, the Ninth Circuit’s holding has provoked disagreement with a California state court. Just a few weeks after the panel issued its original decision, the California Superior Court issued an opinion “disagree[ing]” with the panel’s approach, finding that it “ignore[d] the plain language of the statute by reading a good faith limitation into section 230(c)(2)(B).” *Prager Univ. v. Google LLC*, No. 19CV340667, 2019 WL 8640569, at \*10

(Cal. Super. Ct. Nov. 19, 2019), *appeal docketed*, No. H047714 (Cal. Ct. App. Dec. 19, 2019). That holding led the court to reject a video-maker’s claim that YouTube acted in bad faith by allowing users—such as parents, school administrators, or libraries—to enable a “Restricted Mode” that filters certain sensitive content, such as graphic violence and sexual material. *Id.* at \*2, \*4, \*9-10.

Existing California precedent concerning Section 230 assures that decision will be affirmed. The California Court of Appeal has already held, in a different case, that “Section 230 imposes a subjective element into the [immunity] determination” by conferring immunity “so long as [the developer of the filter] *deemed* the material to be \* \* \* objectionable.” *Pallorium, Inc. v. Jared*, No. G036124, 2007 WL 80955, at \*7 (Cal. Ct. App. Jan. 11, 2007) (emphasis added and internal quotation marks omitted). And that reading comports with the California Supreme Court’s instruction to interpret Section 230 “literally” according to its text. *Barrett v. Rosenthal*, 146 P.3d 510, 529 (Cal. 2006). Thus, there is nothing to be gained by postponing consideration of the question presented. Delay would also be harmful given the high risk of forum shopping: Because California is located within the Ninth Circuit—and home to the Nation’s hub of technological development—plaintiffs now have every incentive to bring suit in federal courts. Certiorari is necessary to eliminate that risk.

## **II. THE QUESTION PRESENTED IS OF SUBSTANTIAL IMPORTANCE.**

Even if the CDA’s text left any ambiguity to be resolved by reference to policy, the Ninth Circuit

profoundly misunderstood how those considerations apply to this case. In fact, the decision below undermines Congress's stated goals in enacting the CDA. It is therefore vital for the Court to address the question presented now. Otherwise, this interpretation will fester—and in the circuit where Section 230 matters the most.

Congress's central goal in enacting Section 230 was to promote a vibrant marketplace to give users tools to provide a safe Internet experience for themselves and their families, without interference by state and federal regulation. By allowing plaintiffs to undermine the immunity granted by Section 230(c)(2)(B) and subjecting filtering-tool providers to prolonged and costly litigation, the Ninth Circuit's opinion accomplishes the opposite by interposing courts as regulators between Internet users and their choice of filtering tools.

Worse still, there is no logical limit to the Ninth Circuit's reasoning. Its ruling invites judges to chip away at all of Section 230(c)'s immunities, including the oft-invoked immunity of 230(c)(1) that protects websites from liability for third-party content. And because the Ninth Circuit's opinion is rooted in policy considerations unmoored from specific statutory text, it invites courts to impose additional policy-driven exceptions beyond the competition context.

**A. The Decision Below Threatens The User Choice And Internet Security Goals That Motivated Section 230(c)(2)(B).**

1. Congress's goal in enacting Section 230, and especially 230(c)(2)(B), was to put Internet users in

the driver's seat of their own online experience by allowing them to choose the filtering tools that best fit their needs without government interference. Congress recognized that services such as Malwarebytes's "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," and that the "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)(2), (4). Congress thus declared that "the policy of the United States" is "to preserve the vibrant and competitive free market that presently exists for the Internet \* \* \*, unfettered by Federal or State regulation"; "to encourage the development of technologies which maximize user control over what information is received"; and "to remove disincentives for the development and utilization of blocking and filtering technologies." *Id.* § 230(b)(2)-(4). As one of the bill's co-sponsors, Representative Chris Cox, explained, "every one of us will be able to tailor what we see to our own tastes" based on Section 230's promotion of a vibrant free market in filtering technology. 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox). In fact, Section 230 was introduced as a user-driven alternative to a bill that sought to combat offensive content through top-down government regulation. *See* Pet. App. 9a-11a.<sup>6</sup>

---

<sup>6</sup> Both provisions were enacted, but Section 230's government-regulation-based rival was largely invalidated by this Court for

As Judge Wilkinson put it in the first major circuit court decision on Section 230—since widely adopted by other courts—Congress created a “broad immunity” “to encourage service providers to self-regulate the dissemination of offensive material.” *Zeran*, 129 F.3d at 331; *accord Jane Doe No. 1*, 817 F.3d at 29 (“Congress did not sound an uncertain trumpet when it enacted the CDA, and it chose to grant broad protections \* \* \*. Showing that a website operates through a meretricious business model is not enough to strip away those protections.”). Part of Congress’s motivation was to overrule a New York state court opinion, under which “computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher.” *Zeran*, 129 F.3d at 331 (discussing *Stratton Oakmont*, 1995 WL 323710); *see also* Pet. App. 9a-10a; H.R. Conf. Rep. No. 104-458, at 194 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 10, 208. The statutory findings, policy statements, and legislative history thus all indicate a desire to let the market, and not courts, decide how content should be filtered.

But the Ninth Circuit’s decision upsets the immunity that Congress created to achieve that goal. In place of the “broad immunity” prescribed by Congress, the Ninth Circuit has authorized courts to abrogate immunity for filtering decisions that, in the

---

violating the First Amendment. *See Reno v. ACLU*, 521 U.S. 844, 877-879 (1997).

court's opinion, Congress would not have wanted to protect. *See* Pet. App. 22a. Under that reasoning, any plaintiff can potentially convince a court to craft an exception for a particular set of facts or alleged motivation, thereby exposing the defendant to the whole panoply of state and federal statutory and common law causes of action that Congress sought to preempt. *See id.* at 13a-14a. So much for providers of filtering tools being “unfettered by Federal or State regulation.” 47 U.S.C. § 230(b)(2).

2. The possibility that a defendant will ultimately prove that it acted with motives a court would consider pure is little comfort. Congress created an *immunity* from suit precisely because, as Judge Wilkinson observed, it “recognized the threat that tort-based lawsuits pose” and so enacted Section 230 “to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.” *Zeran*, 129 F.3d at 330. As the same court later elaborated, “immunity is an *immunity from suit* rather than a mere defense to liability and it is effectively lost if a case is erroneously permitted to go to trial.” *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009) (internal quotation marks omitted). For that reason, “Section 230 immunity” should be “accorded effect at the first logical point in the litigation process.” *Id.* In other contexts, this Court has recognized that immunities are not “merely \*\*\* a defense to monetary liability,” but rather “an immunity from suit” altogether, *Fed. Mar. Comm’n v. S.C. State Ports Auth.*, 535 U.S. 743, 766 (2002) (sovereign immunity), and “an entitlement not to

stand trial or face the other burdens of litigation,” *Mitchell v. Forsyth*, 472 U.S. 511, 526 (1985) (qualified immunity).

If not afforded immunity from suit altogether, Internet services will “face death by ten thousand duck-bites.” *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc). That is why “section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.” *Id.* at 1175.

The danger of abusive litigation in this area is no idle threat. That is because litigious malware purveyors can easily use the exception recognized by the Ninth Circuit to plead around Section 230(c)(2)(B) at the motion-to-dismiss stage. The decision below exacerbates that problem by setting a low bar for what a putative competitor must allege. *See* Pet. App. 23a (accepting Enigma’s claims of “anticompetitive” behavior without enumerating specific facts).

It is not difficult for a purveyor of malware to brand themselves as an anti-malware provider by combining purported security features with objectionable material. For example, in an earlier Ninth Circuit case, the plaintiff combined a supposed “[s]pam [b]locker” with noxious adware that bombarded users with pop-up ads. *Zango*, 568 F.3d at 1170. After the decision below, any purveyor of malware and adware now has a playbook to overcome Section 230(c)(2)(B) simply by adding a purported security feature to their obnoxious software.

Even if the text of Section 230(c)(2)(B) gave courts license to second-guess the motivations for internet-



security firms' classification decisions, judges would be poorly positioned to do so. There are numerous valid reasons Internet-security firms may flag putatively competitive software as a threat. Even well-known brands have had security vulnerabilities or unexpectedly caused computers to slow down,<sup>7</sup> which could justify a potentially-unwanted-program label. More pernicious is fake antivirus software, a common problem that has been a target of government enforcement. Examples include a \$163 million judgment the FTC obtained against an outfit that sold "scareware" to "trick consumers into thinking their computers were infected with malicious software, and then sold them software to 'fix' their non-existent problem"<sup>8</sup>; as well as a \$35 million settlement with the well-known retailer Office Depot for marketing similar "scamware" that "tricked customers into buying millions of dollars' worth of computer repair and technical services by deceptively claiming their software had found malware symptoms on the customers' computers."<sup>9</sup> These firms could write a

---

<sup>7</sup> See, e.g., Eric Griffith, *How to Rid a New PC of Crapware*, PCMag (Apr. 1, 2020), <https://bit.ly/3ch9BMM> (explaining that a well-known antivirus program is "likely to slow [a user's] PC").

<sup>8</sup> Press Release, FTC, *FTC Case Results in \$163 Million Judgment Against "Scareware" Marketer* (Oct. 2, 2012), <https://bit.ly/3bjkJIx>.

<sup>9</sup> Press Release, FTC, *Office Depot and Tech Support Firm Will Pay \$35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services* (Mar. 27, 2019), <https://bit.ly/3afWpWH>.

self-serving complaint like Enigma's to circumvent Section 230(c)(2)(B)'s immunity for cybersecurity firms that seek to protect consumers from these threats.

3. Congress instead intended consumers and their cybersecurity providers to evaluate Internet threats for themselves. By inviting courts to interpose themselves between consumers and cybersecurity services, the Ninth Circuit's decision threatens consumer choice and Internet security.

Purported "competitors" may in fact be legitimate threats to Internet users. *See supra* p. 26 & n.8. Moreover, with millions of potential threats on the Internet, it is impossible for filtering-software companies to individually analyze every potential danger to users. As the Electronic Frontier Foundation (EFF) and CAUCE North America, Inc. explained below, filtering software requires the use of automated algorithms to predict threats, which may sometimes flag potentially competitive software. EFF et al. C.A. *Amicus* Br. 9-10; *see also* ESET, LLC C.A. *Amicus* Br. 7-8 (explaining that Malwarebytes's competitor ESET "encounter[s] more than 300,000 new unique and suspicious objects every day" and that "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 Ninth Circuit's decision puts cybersecurity firms in a predicament. They can try their best to protect consumers against all threats, knowing that they will subject themselves to expensive lawsuits when they designate an alleged competitor as a

threat—either forcing them out of business or raising prices for consumers. Or they can avoid liability by taking a more permissive stance, exposing customers to threats. In either case, consumers end up with an inferior Internet experience. And facing such a choice, new firms may be dissuaded from entering the cybersecurity market altogether—exactly the opposite of what Congress wanted.

There is no need for those dire results. Section 230 has worked just as Congress intended to promote competition in filtering technology. Enigma’s own complaint identified over 40 competing cybersecurity companies. C.A. E.R. 39.<sup>10</sup> The Ninth Circuit’s justification for its policy-driven exception to Section 230(c)(2)(B) was a fear that such firms would “act for their own, and not the public, benefit” by adopting “filtering practices aimed at suppressing competition, rather than protecting internet users.” Pet. App. 20a. In the “vibrant and competitive free market that presently exists \* \* \* unfettered by Federal or State regulation,” 47 U.S.C. § 230(b)(2), however, such a strategy would surely backfire. The reputational damage from self-serving filtering decisions would outweigh the benefits of dissuading a few

---

<sup>10</sup> This shows how unfounded the Ninth Circuit’s competition concerns are in this market. In the antitrust context, such a competitive market would lead to prompt dismissal of any claim that a company had monopoly power. *See, e.g., Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 481 (1992) (giving examples of “nearly 100%,” “80% to 95%,” “87%,” and “over two-thirds” as examples of market shares that could support a monopolization claim).

customers from trying a competitor’s product. And if a customer does find that her cybersecurity provider is not acting in her interest, she has dozens of alternatives to choose from.

**B. The Decision Below Will Undermine Other Tools That Help Internet Users Curate Their Own Online Experience.**

The fallout of the Ninth Circuit’s ruling will not be limited to cybersecurity software. Numerous online services—including tools offered by many of the most commonly used Internet products—are protected by Section 230(c)(2)(B)’s immunity. The Ninth Circuit’s decision, if allowed to stand, will invite lawsuits against these companies’ filtering decisions with ginned-up allegations of anticompetitive motives.

For example, Facebook gives users tools to hide or block content posted by others on their personal Facebook page and has successfully invoked Section 230(c)(2)(B) to defend those tools.<sup>11</sup> YouTube offers users “Restricted Mode”: “an optional setting that you can use on YouTube to help screen out potentially mature content that you may prefer not to see or don’t want others using your device to see.”<sup>12</sup> Likewise, Twitter offers users a “quality filter” that allows them to “filter[] lower-quality content from [their] notifications,” and it gives users tools to limit

---

<sup>11</sup> *Fehrenbach v. Zeldin*, No. 17-CV-5282 (JFB) (ARL), 2018 WL 4242452, at \*5 (E.D.N.Y. Aug. 6, 2018), *report and recommendation adopted*, 2018 WL 4242453 (E.D.N.Y. Sept. 5, 2018).

<sup>12</sup> YouTube Help, *Disable or enable Restricted Mode*, Google, <https://bit.ly/2KftqaQ> (last visited May 11, 2020).

who can send them direct messages and to screen messages with “potentially sensitive” content.<sup>13</sup> Popular message-board website Reddit’s entire content-moderation program relies on “[v]olunteer community moderators” who use Reddit-provided tools “to remove any post that does not follow their community’s rules, without any involvement or direction from Reddit, Inc.”<sup>14</sup>

These are all examples of tools that make the Internet a safer and more pleasant place for consumers. They are just the types of “action taken to enable \* \* \* the technical means to restrict access to material” that Section 230(c)(2)(B) was meant to immunize. 47 U.S.C. § 230(c)(2)(B).

Yet under the Ninth Circuit’s decision, Section 230(c)(2)(B) would no longer provide the kind of absolute immunity Congress intended “to encourage the development of technologies which maximize user control.” *Id.* § 230(b)(3). Rather, plaintiffs whose content is flagged by these tools may write themselves an exception to Section 230(c)(2)(B) by alleging that YouTube or Reddit or Twitter acted with anticompetitive animus towards their content. Indeed, that is exactly what the plaintiff alleged in

---

<sup>13</sup> *About the Notifications timeline*, Twitter, <https://bit.ly/3eu7VRv> (last visited May 11, 2020); *About Direct Messages*, Twitter, <https://bit.ly/3bldCQ2> (last visited May 11, 2020).

<sup>14</sup> *Transparency Report 2019*, Reddit, <https://bit.ly/2ysFhj9> (last visited May 11, 2020) (showing that most removals are by user-moderators using Reddit-provided tools).

*Prager*, *supra* pp. 19-20, the decision that expressly disagreed with the Ninth Circuit's holding here.

**C. The Decision Below Endangers All Of Section 230's Important Immunities.**

The logic of the Ninth Circuit's decision also applies naturally to the rest of Section 230(c)'s immunities and will give courts license to imply additional exceptions beyond one for anticompetitive animus. The opinion's reasoning thus invites replacing the "broad immunity" that "Congress enacted," *Zeran*, 129 F.3d at 331, with an unpredictable quasi-immunity riddled with holes derived from judicial policy preferences.

1. Most obviously, any exception read into Section 230(c)(2)(B) would almost certainly apply to Section 230(c)(2)(A). After all, the "material" to which subsection (c)(2)(B) applies merely incorporates subsection (c)(2)(A)'s list by reference. Moreover, because subsection (c)(2)(A) has the "good faith" condition that (c)(2)(B) lacks, *see supra* pp. 14-15, any exception read into (c)(2)(B) would apply even more readily to (c)(2)(A).

But subsection (c)(2)(A) is crucial to what Congress intended when it enacted subsection (c) as a "[p]rotection for 'Good Samaritan' blocking and screening of offensive material." 47 U.S.C. § 230(c). As Judge Easterbook has explained, Section 230(c)(2) accomplishes that goal by working as a "safety net"; a "web host that \* \* \* filter[s] out offensive material is not liable to the censored customer," thereby "induc[ing] web hosts \* \* \* to take more care to protect the privacy and sensibilities of third parties." *Doe v. GTE Corp.*, 347 F.3d 655, 659-660 (7th Cir.

2003). That goal is understandable: An Internet where services like Facebook, YouTube, and Twitter could not screen graphically violent and sexual content for fear of facing massive litigation costs would be a scary place.

Yet the Ninth Circuit’s insertion of atextual exceptions into Section 230(c)(2) will *discourage* moderation and restore the legal regime Congress intended to overturn with Section 230, in which content moderation creates liability. *See supra* p. 23. “Content moderation at scale is impossible to do well” because of the sheer complexity: services like Facebook receive hundreds of millions of uploads every day, requiring imperfect mass-automated moderation supported by thousands of human judgment calls.<sup>15</sup> Predictably, most anyone whose content is restricted will be upset. Under the Ninth Circuit’s reasoning, so long as that person can come up with plausible allegations that the web service restricted the content in order to favor some competing content, the defendant will be unable to successfully invoke Section 230(c)(2) immunity at the motion-to-dismiss stage. Knowing that Section 230(c)(2) will offer only modest protection against litigious content-providers, interactive computer services will have a tremendous

---

<sup>15</sup> Mike Masnick, *Masnick’s Impossibility Theorem: Content Moderation At Scale Is Impossible To Do Well*, TechDirt (Nov. 20, 2019), <https://bit.ly/2z1XpRh>; see Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv. L. Rev. 1598, 1635-48 (2018) (describing Facebook’s multi-tiered, highly-complex moderation system).

incentive to scale back content moderation—exactly the opposite of the outcome Congress intended.

For example, Facebook’s Community Standards include the platform’s restrictions on hate speech, violent and graphic content, nudity and sexual activity, and sexual solicitation—all under the heading of “*Objectionable Content*.”<sup>16</sup> That is the exact term used in Section 230(c)(2)’s catch-all provision. If courts fashion carve-outs to Section 230(c)(2) immunity for restricting “objectionable” content, purveyors of the most unpleasant software and material could fashion an exception for themselves.

2. The decision below also risks infecting the neighboring immunity in Section 230(c)(1). Whereas subsection (c)(2) immunizes actions to restrict or take down content, subsection (c)(1) immunizes the decision to leave up third-party content. Because the Ninth Circuit’s purposive reasoning was not tethered to any text in (c)(2) and implied an exception from the findings and policy statements that apply to all of Section 230, there is nothing stopping plaintiffs from asking courts to fashion the same exception for (c)(1).

Subsection (c)(1) has been credited by many as having “[c]reated the Internet” as we know it today. *See, e.g.*, Jeff Kosseff, *The Twenty-Six Words That Created the Internet* 4 (2019) (explaining that nine of the ten most popular websites in the United States

---

<sup>16</sup> *Community Standards: Part III. Objectionable Content*, Facebook, <https://bit.ly/2KgiUAq> (last visited May 11, 2020) (emphasis added).



principally publish third-party content and so rely on Section 230(c)(1)). The vibrant Internet we know will be imperiled when plaintiffs seek to circumvent Section 230(c)(1)'s protections using the approach adopted by the Ninth Circuit below.

3. The fallout from the decision below is also not limited to anticompetitive motivation. Following in its logical footsteps, plaintiffs will ask courts to imply other exceptions based on the broad language in the findings and policy statements of Section 230(a) and (b). Prominent U.S. Senators have already done so, suggesting that subsection (a)(3)'s finding that “[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse” should be read to imply an immunity exception if a defendant’s content moderation is not viewpoint-neutral.<sup>17</sup>

If plaintiffs can persuade judges that an Internet service is not providing “educational and informational resources” or “unique opportunities for cultural development,” 47 U.S.C. § 230(a)(1), (3), or is not “promot[ing] the continued development of the Internet,” *id.* § 230(b)(1), will the defendant lose Section 230 immunity? Such potentially far-reaching

---

<sup>17</sup> See Press Release, Senator Ted Cruz, *Sen. Cruz: The Pattern of Political Censorship Seen Across Technology Companies is Highly Concerning* (Jan. 17, 2018), <https://bit.ly/2zdfuMB> (Sen. Cruz committee-hearing comment suggesting that “if you are not a neutral public forum,” then “the entire predicate for liability immunity” under Section 230 is not satisfied); Senator Josh Hawley (@HawleyMO), Twitter (Nov. 27, 2018, 1:22 PM), <https://bit.ly/2VB3CLQ> (suggesting same).

arguments will be hard to distinguish from the Ninth Circuit's use of the policy statements to limit the scope of immunity in this case.

**III. THIS CASE IS AN IDEAL VEHICLE TO RESOLVE THE QUESTION PRESENTED, AND OTHER OPPORTUNITIES MAY NOT SOON PRESENT THEMSELVES.**

1. This case presents an important and purely legal question to the Court without any complicating factual or procedural issues. The Ninth Circuit's ruling that Enigma's complaint should survive dismissal hinges entirely on a straightforward question of statutory interpretation about the scope of Section 230(c)(2)(B)'s immunity. That is an important question that is cleanly presented for this Court to answer.

2. Moreover, this Court may not soon get a better chance to answer the question presented. As the framers of Section 230 recognized, the cost of litigation may itself be enough to force defendants to settle. *See supra* pp. 5-6, 24-29. When facing onerous discovery and legal fees, providers like Malwarebytes may well have to capitulate to plaintiffs' demands not to be marked as threats, making the Internet a more dangerous place for consumers and depriving courts of the ability to provide further guidance on Section 230's immunities. If the Ninth Circuit's atextual exceptions leak into the surrounding provisions of Section 230, *see supra* pp. 31-34, Internet platforms deciding whether to filter offensive content or whether to remove third-party content challenged by a litigious plaintiff will have

similar incentives to settle rather than bear the cost of litigation.

Those dangers are especially heightened because of the Ninth Circuit's outsized role in the technology and Internet sphere. The decision below severely limited the main precedent that scholars have credited with dissuading suits nationwide against companies providing filtering tools.<sup>18</sup> Because so many technology companies are based within the Ninth Circuit, plaintiffs will often have the ability and incentive to bring suit in that circuit, minimizing the chances that another court of appeals or state court will be presented with the same question.

In short, by the time this Court is presented with another opportunity to evaluate whether Section 230 allows judge-made, policy-based exceptions, there is a great danger that filtering-software providers and others who rely on Section 230 will already have modified their business practices in response to the decision below, making the Internet a less safe and vibrant place for consumers.

---

<sup>18</sup> See Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 Tulane J. Tech. & Intell. Prop. 1, 6-7 (2017).

**CONCLUSION**

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

TYLER GRIFFIN NEWBY  
FENWICK & WEST LLP  
555 California Street  
12th Floor  
San Francisco, CA 94104

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

*Counsel for Petitioner*

MAY 2020

## **APPENDIX**

1a

**APPENDIX A**

---

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

No. 17-17351

---

ENIGMA SOFTWARE GROUP USA, LLC,  
*Plaintiff-Appellant,*

v.

MALWAREBYTES, INC.,  
*Defendant-Appellee.*

---

Appeal from the United States District Court  
for the Northern District of California  
Edward J. Davila, District Judge, Presiding

Argued and Submitted February 15, 2019  
San Francisco, California

Filed September 12, 2019  
Amended December 31, 2019

Before: Mary M. Schroeder and Johnnie B.  
Rawlinson, Circuit Judges, and Robert S. Lasnik,\*  
District Judge.

Opinion by Judge SCHROEDER  
Dissent by Judge RAWLINSON

---

\* The Honorable Robert S. Lasnik, United States District Judge for the Western District of Washington, sitting by designation.

---

**SUMMARY\*\***

---

**Communications Decency Act**

The panel filed (1) an order withdrawing its opinion and replacing the opinion with an amended opinion, denying a petition for panel rehearing, and denying on behalf of the court a petition for rehearing en banc; and (2) an amended opinion reversing the district court's dismissal, as barred by § 230 of the Communications Decency Act, of claims under New York law and the Lanham Act's false advertising provision.

Enigma Software Group USA, LLC, and Malwarebytes, Inc., were providers of software that helped internet users to filter unwanted content from their computers. Enigma alleged that Malwarebytes configured its software to block users from accessing Enigma's software in order to divert Enigma's customers.

Section 230, the so-called "Good Samaritan" provision of the Communications Decency Act, immunizes software providers from liability for actions taken to help users block certain types of unwanted online material, including material that is of a violent or sexual nature or is "otherwise objectionable." Distinguishing *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009),

---

\*\* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

the panel held that the phrase “otherwise objectionable” does not include software that the provider finds objectionable for anticompetitive reasons. As to the state-law claims, the panel held that Enigma’s allegations of anticompetitive animus were sufficient to withstand dismissal. As to the federal claim, the panel further held that § 230’s exception for intellectual property claims did not apply because this false advertising claim did not relate to trademarks or any other type of intellectual property. The panel remanded the case for further proceedings.

Dissenting, Judge Rawlinson wrote that § 230 is broadly worded, and Enigma did not persuasively make a case for limitation of the statute beyond its provisions.

---

### COUNSEL

Terry Budd (argued), Budd Law PLLC, Wexford, Pennsylvania; Christopher M. Verdini and Anna Shabalov, K&L Gates LLP, Pittsburgh, Pennsylvania; Edward P. Sangster, K&L Gates LLP, San Francisco, California; for Plaintiff-Appellant.

Tyler G. Newby (argued), Guinevere L. Jobson, and Sapna Mehta, Fenwick & West LLP, San Francisco, California; Benjamin A. Field, Neal Kumar Katyal, and Reedy Swanson, Hogan Lovells US LLP, Washington, D.C; for Defendant-Appellee.

Sophia Cope and Aaron Mackey, Electronic Frontier Foundation, San Francisco, California, for Amici Curiae Electronic Frontier Foundation and CAUCE North America.



Venkat Balasubramani, Focal PLLC, Seattle, Washington; Eric Goldman, Professor; Jess Miers, Law Student; Santa Clara University School of Law, Santa Clara, California; for Amici Curiae Cybersecurity Law Professors.

Anna-Rose Mathieson and Charles Kagay, California Appellate Law Group LLP, San Francisco, California, for Amicus Curiae ESET, LLC.

Brian M. Willen, Wilson Sonsini Goodrich & Rosati, New York, New York; Lauren Gallo White, Wilson Sonsini Goodrich & Rosati, San Francisco, California; for Amicus Curiae Internet Association.

---

### **ORDER**

The opinion filed September 12, 2019 (Docket Entry No. 42), and appearing at 938 F.3d 1026, is withdrawn and replaced by an amended opinion concurrently filed with this order.

With these amendments, Judge Rawlinson voted to grant the petition for panel rehearing. Judges Schroeder and Lasnik voted to deny the petition for panel rehearing. Judge Rawlinson voted to grant the petition for rehearing en banc. Judges Schroeder and Lasnik recommended denying the petition for rehearing en banc.

The full court has been advised of the petition for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for rehearing and petition for rehearing en banc are **DENIED**. No further petitions

for rehearing or rehearing en banc will be entertained.

---

## OPINION

SCHROEDER, Circuit Judge:

### OVERVIEW

This dispute concerns § 230, the so-called “Good Samaritan” provision of the Communications Decency Act of 1996, enacted primarily to protect minors from harmful online viewing. The provision immunizes computer-software providers from liability for actions taken to help users block certain types of unwanted, online material. The provision expressly describes material of a violent or sexual nature, but also includes a catchall for material that is “otherwise objectionable.” 47 U.S.C. § 230(c)(2). We have previously recognized that the provision establishes a subjective standard whereby internet users and software providers decide what online material is objectionable. *See Zango Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 (9th Cir. 2009).

The parties to this dispute are both providers of software that help internet users filter unwanted content from their computers. Plaintiff-Appellant Enigma Software Group USA, LLC has alleged violations of New York state law and a violation of the Lanham Act’s false advertising provision. Each claim is based on the allegation that defendant, Malwarebytes Inc., has configured its software to block users from accessing Enigma’s software in order to divert Enigma’s customers. The district court, relying on *Zango*, dismissed the action as

barred by § 230's broad recognition of immunity. We did not hold in *Zango*, however, that the immunity was limitless.

This case differs from *Zango* in that here the parties are competitors. In this appeal Enigma contends that the "otherwise objectionable" catchall is not broad enough to encompass a provider's objection to a rival's software in order to suppress competition. Enigma points to Judge Fisher's concurrence in *Zango* warning against an overly expansive interpretation of the provision that could lead to anticompetitive results. We heed that warning and reverse the district court's decision that read *Zango* to require such an interpretation. We hold that the phrase "otherwise objectionable" does not include software that the provider finds objectionable for anticompetitive reasons.

Malwarebytes contends that it had legitimate reasons for finding Enigma's software objectionable apart from any anticompetitive effect, and that immunity should therefore apply on Enigma's state-law claims, even if the district court erred in its interpretation of *Zango*. We conclude, however, that Enigma's allegations of anticompetitive animus are sufficient to withstand dismissal.

Enigma's federal claim warrants an additional analytical step. The CDA's immunity provision contains an exception for intellectual property claims, stating that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). Enigma has brought a false advertising claim under the Lanham Act, a federal statute that deals with

trademarks. Enigma contends that the false advertising claim is one “pertaining to intellectual property” and thus outside the scope of § 230 immunity.

Although it is true that the Lanham Act itself deals with intellectual property, *i.e.* trademarks, Enigma’s false advertising claim does not relate to trademarks or any other type of intellectual property. The district court therefore correctly held that the intellectual property exception to immunity does not apply to the false advertising claim. The district court went on to hold that under *Zango’s* application of § 230 immunity, Malwarebytes was immune from liability for false advertising. As with Enigma’s state law claims, we hold that the district court read *Zango* too broadly in dismissing the federal claim. We therefore reverse the judgment on this claim as well.

### **STATUTORY BACKGROUND**

This appeal centers on the immunity provision contained in § 230(c)(2) of the Communications Decency Act (“CDA”), 47 U.S.C. § 230(c)(1996). The CDA, which was enacted as part of the Telecommunications Act of 1996, contains this “Good Samaritan” provision that, in subparagraph B, immunizes internet-service providers from liability for giving internet users the technical means to restrict access to the types of material described in the subparagraph A. *Id.* § 230(c)(2)(B). The material, as described in that subparagraph, is “material that the provider or user considers to be obscene, lewd,

lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” *Id.* § 230(c)(2)(A).<sup>1</sup>

This grant of immunity dates back to the early days of the internet when concerns first arose about children being able to access online pornography. Parents could not program their computers to block online pornography, and this was at least partially due to a combination of trial court decisions in New York that had deterred the creation of online-filtration efforts. In the first case, *Cubby, Inc. v. CompuServe, Inc.*, a federal court held that passive providers of online services and content were not charged with knowledge of, or responsibility for, the content on their network. *See* 776 F. Supp. 135, 139–43 (S.D.N.Y. 1991). Therefore, if a provider remained passive and uninvolved in filtering third-party material from its network, the provider could not be

---

<sup>1</sup> Section 230(c) is entitled “Protection for ‘Good Samaritan’ blocking and screening of offensive material.” The relevant subsection (2), “Civil liability,” states, in full, as follows:

“No provider or user of an interactive computer service shall be held liable on account of –

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph [A].”

47 U.S.C. § 230(c)(2)(A), (B).

held liable for any offensive content it carried from third parties. *See id.*

The corollary of this rule, as later articulated by a New York state trial court, was that once a service provider undertook to filter offensive content from its network, it assumed responsibility for any offensive content it failed to filter, even if it lacked knowledge of the content. *See Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710, \*5 (N.Y. Sup. Ct. May 24, 1995) (“Prodigy’s conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.”), *superseded by statute*, Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 137, *as recognized in Shiamili v. Real Estate Group of N.Y., Inc.*, 952 N.E.2d 1011 (2011). Representative Chris Cox warned during debates on proposed legislation aimed at overruling *Stratton Oakmont*, that premising liability on providers’ efforts to filter out offensive material was deterring software companies from providing the filtering software and tools that could help parents block pornography and other offensive material from their home computers. *See* 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox).

The *Stratton Oakmont* decision, along with the increasing public concern about pornography on the internet, served as catalysts for legislators to consider greater internet regulation. Congress considered, in early 1995, two different amendments to the Telecommunications Act. The first, called the Exon-Coats amendment, targeted pornography at the source by prohibiting its dissemination. *See id.* at 16,068. Proponents of this bill argued that parents

lacked the technological sophistication needed to implement online-filtration tools and that the government therefore needed to step in. *Id.* at 16,099. The second proposal, entitled the Online Family Empowerment Act (“OFEA”), targeted internet pornography at the receiving end by encouraging further development of filtration tools. *Id.* at 22,044. Proponents of this bill pointed out that prohibiting pornography at the source raised constitutional issues involving prior restraint, and argued that parents, not government bureaucrats, were better positioned to protect their children from offensive online material. *Id.* at 16,013.

On February 1, 1996, Congress enacted both approaches as part of the CDA. The Exon-Coats amendment was codified at 47 U.S.C. § 223, but was later invalidated by *Reno v. ACLU*, 521 U.S. 844, 877–79 (1997). Before us is OFEA’s approach, enacted as § 230(c)(2) of the CDA. *See* Pub L. No. 104-104, § 509, 110 Stat. 56, 137–39. By immunizing internet-service providers from liability for any action taken to block, or help users block offensive and objectionable online content, Congress overruled *Stratton Oakmont* and thereby encouraged the development of more sophisticated methods of online filtration. *See* H.R. Conf. Rep. No. 104879, at 194 (1996).

The history of § 230(c)(2) shows that access to pornography was Congress’s motivating concern, but the language used in § 230 included much more, covering any online material considered to be “excessively violent, harassing, or otherwise objectionable.” *See* 47 U.S.C. § 230(c)(2)(A)–(B). Perhaps to guide the interpretation of this broad

language, Congress took the rather unusual step of setting forth policy goals in the immediately preceding paragraph of the statute. *See id.* § 230(b). Of the five goals, three are particularly relevant here. These goals were “to encourage the development of technologies which maximize user control”; “to empower parents to restrict their children’s access to objectionable or inappropriate online content”; and “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services.” *See id.* § 230(b)(2)–(4).

This court has decided one prior case where we considered the scope of § 230, but were principally concerned with which types of online-service providers Congress intended to immunize. *See Zango*, 568 F.3d at 1175. We acknowledged that providers of computer security software can benefit from § 230 immunity, and that such providers have discretion to identify what online content is considered “objectionable,” *id.*, but we had no reason to discuss the scope of that discretion. The separate concurrence in *Zango* focused on the future need for considering appropriate limitations on provider control. *See id.* at 1178–80 (Fisher, J. concurring). District courts have differed in their interpretations of *Zango* and the discretion granted to providers. What is clear to us from the statutory language, history, and case law is that providers do not have unfettered discretion to declare online content “objectionable” and blocking and filtering decisions that are driven by anticompetitive animus are not entitled to immunity under section 230(c)(2).



***FACTUAL BACKGROUND***

Plaintiff-appellant Enigma Software Group USA, LLC, is a Florida company that sells computer security software nationwide. Malwarebytes Inc., a Delaware corporation headquartered in California, also sells computer security software nationwide. Malwarebytes and Enigma are therefore direct competitors.

Providers of computer security software help users identify and block malicious or threatening software, termed malware, from their computers. Each provider generates its own criteria to determine what software might threaten users. Defendant Malwarebytes programs its software to search for what it calls Potentially Unwanted Programs (“PUPs”). PUPs include, for example, what Malwarebytes describes as software that contains “obtrusive, misleading, or deceptive advertisements, branding or search practices.” Once Malwarebytes’s security software is purchased and installed on a user’s computer, it scans for PUPs, and according to Enigma’s complaint, if the user tries to download a program that Malwarebytes has determined to be a PUP, a pop-up alert warns the user of a security risk and advises the user to stop the download and block the potentially threatening content.

Malwarebytes and Enigma have been direct competitors since 2008, the year of Malwarebytes’s inception. In their first eight years as competitors, neither Enigma nor Malwarebytes flagged the other’s software as threatening or unwanted. In late 2016, however, Malwarebytes revised its PUP-detection criteria to include any program that,

according to Malwarebytes, users did not seem to like.

After the revision, Malwarebytes's software immediately began flagging Enigma's most popular programs — RegHunter and SpyHunter — as PUPs. Thereafter, anytime a user with Malwarebytes's software tried to download those Enigma programs, the user was alerted of a security risk and, according to Enigma's complaint, the download was prohibited, *i.e.* Malwarebytes "quarantined" the programs. Enigma alleges that Malwarebytes's new definition of a PUP includes subjective criteria that Malwarebytes has "implemented at its own malicious whim" in order to identify Enigma's programs as threats. Enigma characterizes the revision as a "guise" for anticompetitive conduct, and alleges that its programs are "legitimate", "highly regarded", and "pose no security threat." As a result of Malwarebytes's actions, Enigma claims that it has lost customers and revenue and experienced harm to its reputation.

Enigma brought this action against Malwarebytes in early 2017, in the Southern District of New York. Enigma claimed that Malwarebytes has used its PUP-modification process to advance a "bad faith campaign of unfair competition" aimed at "deceiving consumers and interfering with [Enigma's] customer relationships."

Enigma's complaint alleged four claims, three under New York state law and one under federal law. The first state-law claim accused Malwarebytes of using deceptive business practices in violation of New York General Business Law § 349. Enigma's

second and third state-law claims alleged tortious interference with business and contractual relations in violation of New York state common law. The federal claim accused Malwarebytes of making false and misleading statements to deceive consumers into choosing Malwarebytes's security software over Enigma's, in violation of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

Malwarebytes sought a change of venue. Although Enigma maintained that venue was proper in New York because Malwarebytes's conduct affected users and computers within that state, the conduct at issue had national reach. The district court therefore granted Malwarebytes's motion to transfer the case to the Northern District of California, where Malwarebytes is headquartered.

Malwarebytes then moved to dismiss for failure to state a claim, arguing that it was immune from liability under § 230(c)(2) of the CDA. The district court granted the motion, finding that under the reasoning of our decision in *Zango*, Malwarebytes was immune under § 230 on all of Enigma's claims. The district court interpreted *Zango* to mean that anti-malware software providers are free to block users from accessing any material that those providers, in their discretion, deem to be objectionable. Given Malwarebytes's status as a provider of filtering software, and its assertion that Enigma's programs are potentially unwanted, the district court held that Malwarebytes could not be liable under state law for blocking users' access to Enigma's programs.

With respect to the federal claim, the district court had to consider the intellectual property exception to the CDA's immunity provision set forth in 47 U.S.C. § 230(e)(2). The somewhat opaque exception states that § 230 immunity "shall not be construed to limit or expand any law pertaining to intellectual property." *Id.* Enigma's federal claim alleged false advertising under the Lanham Act, and Enigma contended that immunity did not apply because that statute deals with intellectual property, *i.e.* trademarks. The district court reasoned, however, that although the Lanham Act itself deals with intellectual property, Enigma's false advertising claim did not relate to any type of intellectual property and therefore § 230 immunity encompassed that claim as well. Having concluded that Malwarebytes was immune on all four claims, the district court dismissed the complaint and granted judgment for Malwarebytes.

On appeal, Enigma primarily contends that the district court erred in interpreting our *Zango* opinion to give online service providers unlimited discretion to block online content, and that the Good Samaritan blocking provision does not provide such sweeping immunity that it encompasses anticompetitive conduct.

## ***DISCUSSION***

### **I. Scope of § 230(c)(2) Immunity as Applied to State-Law Claims**

The district court held that our opinion in *Zango* controlled, and interpreted *Zango* to mean that an online-service provider cannot be liable for blocking internet users from accessing online content that the

provider considers objectionable, regardless of the provider’s motivations or the harmful effects of the blocking. The scope of the statutory catchall phrase, “otherwise objectionable,” was not at issue in *Zango*, however. The central issue in *Zango* was whether § 230 immunity applies to filtering software providers like the defendant Kaspersky in that case, and both parties in this case. *See* 568 F.3d at 1173, 1176. We held such providers had immunity. *Id.* at 1177–78. At the end of our majority opinion, we emphasized the relevant statutory language in stating that § 230 permits providers to block material “that either the provider *or* the user considers . . . objectionable.” *See id.* at 1177 (original emphasis). The district court focused on that sentence and reasoned that Malwarebytes had unfettered discretion to select what criteria makes a program “objectionable” under § 230, and further, that the court was not to analyze Malwarebytes’s reasons for doing so.

The majority in *Zango* did not, however, address whether there were limitations on a provider’s discretion to declare online content “objectionable.” No such issue was raised in the appeal. We noted that *Zango* “waived” the argument that its software was not “objectionable.” *See id.* at 1176–77. We therefore held that § 230 immunity covered Kaspersky’s decision to block users from accessing the type of content at issue in that case and concluded that § 230 permits providers to block material that “the provider considers . . . objectionable.” *Id.* at 1177.

It was Judge Fisher’s concurring opinion in *Zango* that framed the issue for future litigation as to whether the term “objectionable” might be construed

in a way that would immunize providers even if they blocked online content for improper reasons. *See id.* at 1178–80 (Fisher, J. concurring). Judge Fisher warned that extending immunity beyond the facts of that case could “pose serious problems,” particularly where a provider is charged with using § 230 immunity to advance an anticompetitive agenda. *See id.* at 1178. He said that an “unbounded” reading of the phrase “otherwise objectionable” would allow a content provider to “block content for anticompetitive purposes or merely at its malicious whim.” *Id.*

District courts nationwide have grappled with the issues discussed in *Zango*’s majority and concurring opinions, and have reached differing results. Like the district court in this case, at least two other federal district courts have relied on *Zango* to dismiss software-provider lawsuits against Malwarebytes where the plaintiff claimed that Malwarebytes improperly characterized the plaintiff’s software as a PUP. *See PC Drivers Headquarters, LP v. Malwarebytes Inc.*, 371 F. Supp. 3d 652 (N.D. Cal. 2019); *PC Drivers Headquarters, LP v. Malwarebytes, Inc.*, No. 1:18-CV-234-RP, 2018 WL 2996897, at \*1 (W.D. Tex. Apr. 23, 2018).

Other district courts have viewed our holding in *Zango* to be less expansive. *See Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 884 (N.D. Cal. 2015) (noting that just because “the statute requires the user or service provider to subjectively believe the blocked or screened material is objectionable does not mean anything or everything YouTube finds subjectively objectionable is within the scope of Section 230(c),” and concluding that, “[o]n the contrary such an ‘unbounded’ reading . . . would

enable content providers to ‘block content for anticompetitive reasons[.]’”) (quoting Judge Fisher’s concurrence in *Zango*); *Sherman v. Yahoo! Inc.*, 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014) (same); see also *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. Mar. 11, 2011) (acknowledging that a provider’s subjective determination of what constitutes objectionable material under § 230(c)(2) is not limitless, but finding that the harassing emails in that case were reasonably objectionable).

We find these decisions recognizing limitations in the scope of immunity to be persuasive. The courts interpreting *Zango* as providing unlimited immunity seem to us to have stretched our opinion in *Zango* too far. This is because the focus of that appeal was neither what type of material may be blocked, nor why it may be blocked, but rather who benefits from § 230 immunity. The issue was whether § 230 immunity applies to filtering-software providers. See *Zango*, 568 F.3d at 1173. We answered that question in the affirmative, explaining that Kaspersky was the type of “interactive computer service” to which § 230(c)(2) expressly referred, and that Kaspersky was engaged in the type of conduct to which § 230(c)(2) generally applies. *Id.* at 1175–76.

As relevant here, the majority opinion in *Zango* establishes only that Malwarebytes, as a filtering-software provider, is an entity to which the immunity afforded by § 230 would apply. The majority opinion does not require us to hold that we lack the authority to question Malwarebytes’s determinations of what content to block. We must therefore in this case analyze § 230 to decide what

limitations, if any, there are on the ability of a filtering software provider to block users from receiving online programming.

The legal question before us is whether § 230(c)(2) immunizes blocking and filtering decisions that are driven by anticompetitive animus. The majority in *Zango* had no occasion to address the issue, and the parties in that case were not competitors. *See* 568 F. 3d at 1170 (explaining Kaspersky is a security software provider; Zango provides an online service for users to stream movies, video games, and music). This is the first § 230 case we are aware of that involves direct competitors.

In this appeal, Enigma alleges that Malwarebytes blocked Enigma's programs for anticompetitive reasons, not because the programs' content was objectionable within the meaning of § 230, and that § 230 does not provide immunity for anticompetitive conduct. Malwarebytes's position is that, given the catchall, Malwarebytes has immunity regardless of any anticompetitive motives.

We cannot accept Malwarebytes's position, as it appears contrary to CDA's history and purpose. Congress expressly provided that the CDA aims "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services" and to "remove disincentives for the development and utilization of blocking and filtering technologies." § 230(b)(2)–(3). Congress said it gave providers discretion to identify objectionable content in large part to protect competition, not suppress it. *Id.* In other words, Congress wanted to encourage the development of



filtration technologies, not to enable software developers to drive each other out of business.

In the infancy of the internet, the unwillingness of Congress to spell out the meaning of “otherwise objectionable” was understandable. The broad grant of protective control over online content may have been more readily acceptable in an era before the potential magnitude of internet communication was fully comprehended. Indeed, the fears of harmful content at the time led Congress to enact, in the same statute, an outright ban on the dissemination of online pornography, a ban which the Supreme Court swiftly rejected as unconstitutional a year later. *See Reno v. ACLU*, 521 U.S. at 877–79 (striking down 47 U.S.C. § 223).

We must today recognize that interpreting the statute to give providers unbridled discretion to block online content would, as Judge Fisher warned, enable and potentially motivate internet-service providers to act for their own, and not the public, benefit. *See* 568 F.3d at 1178 (Fisher, J., concurring). Immunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress’s stated policy. *See* § 230(b)(3) (to maximize user control over what content they view). Indeed, users selecting a security software provider must trust that the provider will block material consistent with that user’s desires. Users would not reasonably anticipate providers blocking valuable online content in order to stifle competition. Immunizing anticompetitive blocking would, therefore, be contrary to another of the statute’s express policies:

“removing disincentives for the utilization of blocking and filtering technologies.” *Id.* § 230(b)(4).

We therefore reject Malwarebytes’s position that § 230 immunity applies regardless of anticompetitive purpose. But we cannot, as Enigma asks us to do, ignore the breadth of the term “objectionable” by construing it to cover only material that is sexual or violent in nature. Enigma would have us read the general, catchall phrase “otherwise objectionable” as limited to the categories of online material described in the seven specific categories that precede it. *See* 47 U.S.C. § 230(c)(2) (describing material that is “obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable.”). Enigma argues that its software has no such content, and that Malwarebytes therefore cannot claim immunity for blocking it.

Enigma relies on the principle of *ejusdem generis*, which teaches that when a generic term follows specific terms, the generic term should be construed to reference subjects akin to those with the specific enumeration. *See, e.g., Norfolk & W. Ry. Co. v. Am. Train Dispatchers Ass’n*, 499 U.S. 117, 129 (1991). But the specific categories listed in § 230(c)(2) vary greatly: Material that is lewd or lascivious is not necessarily similar to material that is violent, or material that is harassing. If the enumerated categories are not similar, they provide little or no assistance in interpreting the more general category. We have previously recognized this concept. *See Sacramento Reg’l Cty. Sanitation Dist. v. Reilly*, 905 F.2d 1262, 1270 (9th Cir. 1990) (“Where the list of objects that precedes the ‘or other’ phrase is dissimilar, *ejusdem generis* does not apply”).

We think that the catchall was more likely intended to encapsulate forms of unwanted online content that Congress could not identify in the 1990s. But even if *ejusdem generis* did apply, it would not support Enigma’s narrow interpretation of “otherwise objectionable.” Congress wanted to give internet users tools to avoid not only violent or sexually explicit materials, but also harassing materials. Spam, malware and adware could fairly be placed close enough to harassing materials to at least be called “otherwise objectionable” while still being faithful to the principle of *ejusdem generis*. Several district courts have, for example, regarded unsolicited marketing emails as “objectionable.” *See, e.g., Holomaxx*, 783 F. Supp. 2d at 1104; *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 608–610 (N.D. Ill. 2008); *see also Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, No. CIV09-4567-RBK-KMW, 2010 WL 1799456, at \*6 (D.N.J. May 4, 2010). But we do not, in this appeal, determine the precise relationship between the term “otherwise objectionable” and the seven categories that precede it. We conclude only that if a provider’s basis for objecting to and seeking to block materials is because those materials benefit a competitor, the objection would not fall within any category listed in the statute and the immunity would not apply.

Malwarebytes’s fallback position is that, even if it would lack immunity for anticompetitive blocking, Malwarebytes has found Enigma’s programs “objectionable” for legitimate reasons based on the programs’ content. Malwarebytes asserts that Enigma’s programs, SpyHunter and RegHunter, use “deceptive tactics” to scare users into believing that they have to download Enigma’s programs to prevent

their computers from being infected. Enigma alleges, however, that its programs “pose no security threat” and that Malwarebytes’s justification for blocking these “legitimate” and “highly regarded” programs was a guise for anticompetitive animus.

The district court interpreted our holding in *Zango* to foreclose this debate entirely, implicitly reasoning that if Malwarebytes has sole discretion to select what programs are “objectionable,” the court need not evaluate the reasons for the designation. Because we hold that § 230 does not provide immunity for blocking a competitor’s program for anticompetitive reasons, and because Enigma has specifically alleged that the blocking here was anticompetitive, Enigma’s claims survive the motion to dismiss. We therefore reverse the dismissal of Enigma’s state-law claims and we remand for further proceedings.

## **II. The Federal Claim and the CDA’s Intellectual Property Exception**

Enigma’s fourth claim is a claim for false advertising under the Lanham Act, a statute dealing with a form of intellectual property, *i.e.* trademarks. Enigma alleges that Malwarebytes publicly mischaracterized Enigma’s programs SpyHunter and RegHunter as potentially unwanted or PUPs, and it did so in order to interfere with Enigma’s customer base and divert those customers to Malwarebytes.

Section 230(e)(2) of the CDA contains an exception to immunity for intellectual property claims. *See* 47 U.S.C. § 230(e)(2). This exception, known as the intellectual property carve out, states that § 230 immunity shall not “limit or expand any law pertaining to intellectual property.” *Id.* In light of

that exception, Enigma contends that immunity would not bar Enigma's Lanham Act claim, even if immunity is available to Malwarebytes on the state law claims. Although Enigma's claim does not itself involve an intellectual property right, Enigma characterizes its federal false advertising claim as one "pertaining to intellectual property" within the meaning of § 230(e)(2) because the Lanham Act deals with intellectual property. The district court rejected this argument, and rightly so.

This is because even though the Lanham Act is known as the federal trademark statute, not all claims brought under the statute involve trademarks. The Act contains two parts, one governing trademark infringement and another governing false designations of origin, false descriptions, and dilution. *Compare* 15 U.S.C. § 1114 (trademark infringement) *with id.* § 1125 (the rest). The latter, § 1125, creates two bases of liability, false association and false advertising. *Compare* § 1125(a)(1)(A) (false association) *with* § 1125(a)(1)(B) (false advertising). Thus, although "much of the Lanham Act addresses the registration, use, and infringement of trademarks and related marks, . . . § 1125(a) is one of the few provisions that goes beyond trademark protection." *Dastar Corp. v. Twentieth Cent. Fox Film Corp.*, 539 U.S. 23, 28–29 (2003).

In this appeal, we must decide whether the exception to immunity contained in § 230(e)(2) applies to false advertising claims brought under the Lanham Act. Our court has not addressed the issue, although we have considered the exception as it would apply to state law claims. *See Perfect 10 v.*

*CCBill, LLC*, 488 F.3d 1102, 1118–19 (9th Cir. 2009) (concluding that the intellectual property exception in § 230(e)(2) was not intended to cover intellectual property claims brought under state law); *see also Gen. Steel Domestic Sales, L.L.C. v. Chumley*, 840 F.3d 1178, 1182 (10th Cir. 2016) (declining to analyze the intellectual property exception; explaining that because “§ 230 does not contain the grant of immunity from suit contended for, it is unnecessary to discuss its applicability to the Lanham Act false advertising claims”).

We have observed before that because Congress did not define the term “intellectual property law,” it should be construed narrowly to advance the CDA’s express policy of providing broad immunity. *See Perfect 10*, 488 F.3d at 1119. One of these express policy reasons for providing immunity was, as Congress stated in § 230(b)(2), “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). The intellectual property exception is a limitation on immunity, and the CDA’s stated congressional purpose counsels against an expansive interpretation of the exception that would diminish the scope of immunity. If the intellectual property law exception were to encompass any claim raised under the Lanham Act—including false advertising claims that do not directly involve intellectual property rights—it would create a potential for new liability that would upset, rather than “preserve” the vibrant culture of innovation on the internet that Congress envisioned. *Id.*

We therefore hold that the intellectual property exception contained in § 230(e)(2) encompasses claims pertaining to an established intellectual property right under federal law, like those inherent in a patent, copyright, or trademark. The exception does not apply to false advertising claims brought under § 1125(a) of the Lanham Act, unless the claim itself involves intellectual property.

Here, Enigma's Lanham Act claim derives from the statute's false advertising provision. Enigma alleges that Malwarebytes mischaracterized Enigma's most popular software programs in order to divert Enigma's customers to Malwarebytes. These allegations do not relate to or involve trademark rights or any other intellectual property rights. Thus, Enigma's false advertising claim is not a claim "pertaining to intellectual property law" within the meaning of § 230(e)(2). The district court correctly concluded that the intellectual property exception to immunity does not encompass Enigma's Lanham Act claim.

The district court went on to hold, however, as it did with the state law claims, that Malwarebytes is nevertheless immune from liability under our decision in *Zango*. As we have explained with respect to the state law claims, *Zango* did not define an unlimited scope of immunity under § 230, and immunity under that section does not extend to anticompetitive conduct. Because the federal claim, like the state claims, is based on allegations of such conduct, the federal claim survives dismissal. We therefore reverse the district court's judgment in favor of Malwarebytes and remand for further proceedings on this claim as well.

27a

***CONCLUSION***

The judgment of the district court is reversed and the case is remanded for further proceedings consistent with this opinion.

**REVERSED and REMANDED.**

---



RAWLINSON, Circuit Judge, dissenting:

In his concurring opinion in *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1179–80 (9th Cir. 2009), Judge Fisher acknowledged that “until Congress clarifies the statute or a future litigant makes the case for a possible limitation,” the “broadly worded” Communications Decency Act (the Act) afforded immunity to a distributor of Internet security software. Congress has not further clarified the statute and Enigma Software has not persuasively made a case for limitation of the statute beyond its provisions.

The majority opinion seeks to limit the statute based on the fact that the parties are competitors. *See Majority Opinion*, p. 6. However, nothing in the statutory provisions or our majority opinion in *Zango* supports such a distinction. Rather the “broad language” of the Act specifically encompasses “any action voluntarily taken [by a provider] to restrict access to . . . material that the provider . . . considers to be . . . otherwise objectionable.” 47 U.S.C. § 230(c)(2)(A) (emphasis added). Under the language of the Act, so long as the provider’s action is taken to remove “otherwise objectionable” material, the restriction of access is immunized. *See id.* The majority’s real complaint is not that the district court construed the statute too broadly, but that the statute is written too broadly. However, that defect, if it is a defect, is one beyond our authority to correct. *See Baker Botts LLP v. ASARCO LLC*, 135 S. Ct. 2158, 2169 (2015).

In particular, the majority holds that the criteria for blocking online material may not be based on the

identity of the entity that produced it. *See Majority Opinion*, p. 11. Unfortunately, however, that conclusion cannot be squared with the broad language of the Act. Under the language of the statute, if the blocked content is “otherwise objectionable” to the provider, the Act bestows immunity. *Zango*, 568 F.3d at 1173 (“[T]he statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user *or the provider* deems objectionable.”) (emphasis in the original); 1174 (“According protection to providers of programs that filter adware and malware is also consistent with the Congressional goals for immunity articulated in [47 U.S.C.] § 230 itself.”). Although the parties were not direct competitors, the plaintiff in *Zango* asserted similar anti-competition effects. *See id.* at 1171–72. The majority’s policy arguments are in conflict with our recognition in *Zango* that the broad language of the Act is consistent with “the Congressional goals for immunity” as expressed in the language of the statute. *Id.* at 1174. As the district court cogently noted, we “must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Connecticut Nat’l Bank v. Germain*, 503 U.S. 249, 253–54 (1992) (citations omitted).

I respectfully dissent.

30a

**APPENDIX B**

---

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

No. 17-17351

---

ENIGMA SOFTWARE GROUP USA, LLC,  
*Plaintiff-Appellant,*

v.

MALWAREBYTES, INC.,  
*Defendant-Appellee.*

---

Appeal from the United States District Court  
for the Northern District of California  
Edward J. Davila, District Judge, Presiding

Argued and Submitted February 15, 2019  
San Francisco, California

Filed September 12, 2019

Before: Mary M. Schroeder and Johnnie B.  
Rawlinson, Circuit Judges, and Robert S. Lasnik,\*  
District Judge.

---

\* The Honorable Robert S. Lasnik, United States District Judge  
for the Western District of Washington, sitting by designation.

Opinion by Judge Schroeder;  
Dissent by Judge Rawlinson

---

**SUMMARY\*\***

---

**Communications Decency Act**

The panel reversed the district court’s dismissal, as barred by § 230 of the Communications Decency Act, of claims under New York law and the Lanham Act’s false advertising provision.

Enigma Software Group USA, LLC, and Malwarebytes, Inc., were providers of software that helped internet users to filter unwanted content from their computers. Enigma alleged that Malwarebytes configured its software to block users from accessing Enigma’s software in order to divert Enigma’s customers.

Section 230 immunizes software providers from liability for actions taken to help users block certain types of unwanted online material, including material that is of a violent or sexual nature or is “otherwise objectionable.” Distinguishing *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009), the panel held that the phrase “otherwise objectionable” does not include software that the provider finds objectionable for anticompetitive

---

\*\* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

reasons. As to the state-law claims, the panel held that Enigma’s allegations of anticompetitive animus were sufficient to withstand dismissal. As to the federal claim, the panel further held that § 230’s exception for intellectual property claims did not apply because this false advertising claim did not relate to trademarks or any other type of intellectual property. The panel remanded the case for further proceedings.

Dissenting, Judge Rawlinson wrote that § 230 is broadly worded, and Enigma did not persuasively make a case for limitation of the statute beyond its provisions.

---

### **COUNSEL**

Terry Budd (argued), Budd Law PLLC, Wexford, Pennsylvania; Christopher M. Verdini and Anna Shabalov, K&L Gates LLP, Pittsburgh, Pennsylvania; Edward P. Sangster, K&L Gates LLP, San Francisco, California; for Plaintiff-Appellant.

Tyler G. Newby (argued), Guinevere L. Job son, and Sapna Mehta, Fenwick & West LLP, San Francisco, California, for Defendant-Appellee.

---

### **OPINION**

SCHROEDER, Circuit Judge:

#### ***OVERVIEW***

This dispute concerns § 230, the so-called “Good Samaritan” provision of the Communications Decency Act of 1996, enacted primarily to protect

minors from harmful online viewing. The provision immunizes computer-software providers from liability for actions taken to help users block certain types of unwanted, online material. The provision expressly describes material of a violent or sexual nature, but also includes a catchall for material that is “otherwise objectionable.” 47 U.S.C. § 230(c)(2). We have previously recognized that the provision establishes a subjective standard whereby internet users and software providers decide what online material is objectionable. *See Zango Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 (9th Cir. 2009).

The parties to this dispute are both providers of software that help internet users filter unwanted content from their computers. Plaintiff-Appellant Enigma Software Group USA, LLC has alleged violations of New York state law and a violation of the Lanham Act’s false advertising provision. Each claim is based on the allegation that defendant, Malwarebytes Inc., has configured its software to block users from accessing Enigma’s software in order to divert Enigma’s customers. The district court, relying on *Zango*, dismissed the action as barred by § 230’s broad recognition of immunity. We did not hold in *Zango*, however, that the immunity was limitless.

This case differs from *Zango* in that here the parties are competitors. In this appeal Enigma contends that the “otherwise objectionable” catchall is not broad enough to encompass a provider’s objection to a rival’s software in order to suppress competition. Enigma points to Judge Fisher’s concurrence in *Zango* warning against an overly expansive interpretation of the provision that could

lead to anticompetitive results. We heed that warning and reverse the district court's decision that read *Zango* to require such an interpretation. We hold that the phrase "otherwise objectionable" does not include software that the provider finds objectionable for anticompetitive reasons.

Malwarebytes contends that it had legitimate reasons for finding Enigma's software objectionable apart from any anticompetitive effect, and that immunity should therefore apply on Enigma's state-law claims, even if the district court erred in its interpretation of *Zango*. We conclude, however, that Enigma's allegations of anticompetitive animus are sufficient to withstand dismissal.

Enigma's federal claim warrants an additional analytical step. The CDA's immunity provision contains an exception for intellectual property claims, stating that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). Enigma has brought a false advertising claim under the Lanham Act, a federal statute that deals with trademarks. Enigma contends that the false advertising claim is one "pertaining to intellectual property" and thus outside the scope of § 230 immunity.

Although it is true that the Lanham Act itself deals with intellectual property, *i.e.* trademarks, Enigma's false advertising claim does not relate to trademarks or any other type of intellectual property. The district court therefore correctly held that the intellectual property exception to immunity does not

apply to the false advertising claim. The district court went on to hold that under *Zango's* application of § 230 immunity, Malwarebytes was immune from liability for false advertising. As with Enigma's state law claims, we hold that the district court read *Zango* too broadly in dismissing the federal claim. We therefore reverse the judgment on this claim as well.

### **STATUTORY BACKGROUND**

This appeal centers on the immunity provision contained in § 230(c)(2) of the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1996). The CDA, which was enacted as part of the Telecommunications Act of 1996, contains this "Good Samaritan" provision that, in subparagraph B, immunizes internet-service providers from liability for giving internet users the technical means to restrict access to the types of material described in the subparagraph A. *Id.* § 230(c)(2)(B). The material, as described in that subparagraph, is "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." *Id.* § 230(c)(2)(A).<sup>1</sup>

---

<sup>1</sup> Section 230(c) is entitled "Protection for 'Good Samaritan' blocking and screening of offensive material." The relevant subsection (2), "Civil liability," states, in full, as follows:

"No provider or user of an interactive computer service shall be held liable on account of —

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise



This grant of immunity dates back to the early days of the internet when concerns first arose about children being able to access online pornography. Parents could not program their computers to block online pornography, and this was at least partially due to a combination of trial court decisions in New York that had deterred the creation of online-filtration efforts. In the first case, *Cubby, Inc. v. CompuServe, Inc.*, a federal court held that passive providers of online services and content were not charged with knowledge of, or responsibility for, the content on their network. *See* 776 F. Supp 135, 139-43 (S.D.N.Y. 1991). Therefore, if a provider remained passive and uninvolved in filtering third-party material from its network, the provider could not be held liable for any offensive content it carried from third parties. *See id.*

The corollary of this rule, as later articulated by a New York state trial court, was that once a service provider undertook to filter offensive content from its network, it assumed responsibility for any offensive content it failed to filter, even if it lacked knowledge of the content. *See Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710, \*5 (N.Y. Sup. Ct. May 24, 1995) (“Prodigy’s conscious choice, to gain the benefits of editorial control, has opened it up to a

---

objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph [A].”

47 U.S.C. § 230(c)(2)(A), (B).

greater liability than CompuServe and other computer networks that make no such choice.”), *superseded by statute*, Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 137, *as recognized in Shiamili v. Real Estate Group of N.Y., Inc.*, 952 N.E.2d 1011 (2011). Representative Chris Cox warned during debates on proposed legislation aimed at overruling *Stratton Oakmont*, that premising liability on providers’ efforts to filter out offensive material was deterring software companies from providing the filtering software and tools that could help parents block pornography and other offensive material from their home computers. *See* 141 Cong. Rec. 22,045 (1995) (statement of Rep. Cox).

The *Stratton Oakmont* decision, along with the increasing public concern about pornography on the internet, served as catalysts for legislators to consider greater internet regulation. Congress considered, in early 1995, two different amendments to the Telecommunications Act. The first, called the Exon-Coats amendment, targeted pornography at the source by prohibiting its dissemination. *See id.* at 16,068. Proponents of this bill argued that parents lacked the technological sophistication needed to implement online-filtration tools and that the government therefore needed to step in. *Id.* at 16,099. The second proposal, entitled the Online Family Empowerment Act (“OFEA”), targeted internet pornography at the receiving end by encouraging further development of filtration tools. *Id.* at 22,044. Proponents of this bill pointed out that prohibiting pornography at the source raised constitutional issues involving prior restraint, and argued that parents, not government bureaucrats,

were better positioned to protect their children from offensive online material. *Id.* at 16,013.

On February 1, 1996, Congress enacted both approaches as part of the CDA. The Exon-Coats amendment was codified at 47 U.S.C. § 223, but was later invalidated by *Reno v. ACLU*, 521 U.S. 844, 877-79 (1997). Before us is OFEA's approach, enacted as § 230(c)(2) of the CDA. *See* Pub L. No. 104-104, § 509, 110 Stat. 56, 137-39. By immunizing internet-service providers from liability for any action taken to block, or help users block offensive and objectionable online content, Congress overruled *Stratton Oakmont* and thereby encouraged the development of more sophisticated methods of online filtration. *See* H.R. Conf. Rep. No. 104-879, at 194 (1996).

The history of § 230(c)(2) shows that access to pornography was Congress's motivating concern, but the language used in § 230 included much more, covering any online material considered to be "excessively violent, harassing, or otherwise objectionable." *See* 47 U.S.C. § 230(c)(2)(A)—(B). Perhaps to guide the interpretation of this broad language, Congress took the rather unusual step of setting forth policy goals in the immediately preceding paragraph of the statute. *See id.* § 230(b). Of the five goals, three are particularly relevant here. These goals were "to encourage the development of technologies which maximize user control"; "to empower parents to restrict their children's access to objectionable or inappropriate online content"; and "to preserve the vibrant and competitive free market that presently exists for the

Internet and other interactive computer services.”  
*See id.* § 230(b)(2)—(4).

This court has decided one prior case where we considered the scope of § 230, but were principally concerned with which types of online-service providers Congress intended to immunize. *See Zango*, 568 F.3d at 1175. We acknowledged that providers of computer security software can benefit from § 230 immunity, and that such providers have discretion to identify what online content is considered “objectionable,” *id.*, but we had no reason to discuss the scope of that discretion. The separate concurrence in *Zango* focused on the future need for considering appropriate limitations on provider control. *See id.* at 1178-80 (Fisher, J. concurring). District courts have differed in their interpretations of *Zango* and the extent to which it encouraged providers to block material. What is clear to us from the statutory language, history and case law is that the criteria for blocking online material must be based on the characteristics of the online material, *i.e.* its content, and not on the identity of the entity that produced it.

### ***FACTUAL BACKGROUND***

Plaintiff-appellant Enigma Software Group USA, LLC, is a Florida company that sells computer security software nationwide. Malwarebytes Inc., a Delaware corporation headquartered in California, also sells computer security software nationwide. Malwarebytes and Enigma are therefore direct competitors.

Providers of computer security software help users identify and block malicious or threatening software,

termed malware, from their computers. Each provider generates its own criteria to determine what software might threaten users. Defendant Malwarebytes programs its software to search for what it calls Potentially Unwanted Programs (“PUPs”). PUPs include, for example, what Malwarebytes describes as software that contains “obtrusive, misleading, or deceptive advertisements, branding or search practices.” Once Malwarebytes’s security software is purchased and installed on a user’s computer, it scans for PUPs, and according to Enigma’s complaint, if the user tries to download a program that Malwarebytes has determined to be a PUP, a pop-up alert warns the user of a security risk and advises the user to stop the download and block the potentially threatening content.

Malwarebytes and Enigma have been direct competitors since 2008, the year of Malwarebytes’s inception. In their first eight years as competitors, neither Enigma nor Malwarebytes flagged the other’s software as threatening or unwanted. In late 2016, however, Malwarebytes revised its PUP-detection criteria to include any program that, according to Malwarebytes, users did not seem to like.

After the revision, Malwarebytes’s software immediately began flagging Enigma’s most popular programs—RegHunter and SpyHunter—as PUPs. Thereafter, anytime a user with Malwarebytes’s software tried to download those Enigma programs, the user was alerted of a security risk and, according to Enigma’s complaint, the download was prohibited, *i.e.* Malwarebytes “quarantined” the programs. Enigma alleges that Malwarebytes’s new definition

of a PUP includes subjective criteria that Malwarebytes has “implemented at its own malicious whim” in order to identify Enigma’s programs as threats. Enigma characterizes the revision as a “guise” for anticompetitive conduct, and alleges that its programs are “legitimate”, “highly regarded”, and “pose no security threat.” As a result of Malwarebytes’s actions, Enigma claims that it has lost customers and revenue and experienced harm to its reputation.

Enigma brought this action against Malwarebytes in early 2017, in the Southern District of New York. Enigma claimed that Malwarebytes has used its PUP-modification process to advance a “bad faith campaign of unfair competition” aimed at “deceiving consumers and interfering with [Enigma’s] customer relationships.”

Enigma’s complaint alleged four claims, three under New York state law and one under federal law. The first state-law claim accused Malwarebytes of using deceptive business practices in violation of New York General Business Law § 349. Enigma’s second and third state-law claims alleged tortious interference with business and contractual relations in violation of New York state common law. The federal claim accused Malwarebytes of making false and misleading statements to deceive consumers into choosing Malwarebytes’s security software over Enigma’s, in violation of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

Malwarebytes sought a change of venue. Although Enigma maintained that venue was proper in New York because Malwarebytes’s conduct affected users

and computers within that state, the conduct at issue had national reach. The district court therefore granted Malwarebytes's motion to transfer the case to the Northern District of California, where Malwarebytes is headquartered.

Malwarebytes then moved to dismiss for failure to state a claim, arguing that it was immune from liability under § 230(c)(2) of the CDA. The district court granted the motion, finding that under the reasoning of our decision in *Zango*, Malwarebytes was immune under § 230 on all of Enigma's claims. The district court interpreted *Zango* to mean that anti-malware software providers are free to block users from accessing any material that those providers, in their discretion, deem to be objectionable. Given Malwarebytes's status as a provider of filtering software, and its assertion that Enigma's programs are potentially unwanted, the district court held that Malwarebytes could not be liable under state law for blocking users' access to Enigma's programs.

With respect to the federal claim, the district court had to consider the intellectual property exception to the CDA's immunity provision set forth in 47 U.S.C. § 230(e)(2). The somewhat opaque exception states that § 230 immunity "shall not be construed to limit or expand any law pertaining to intellectual property." *Id.* Enigma's federal claim alleged false advertising under the Lanham Act, and Enigma contended that immunity did not apply because that statute deals with intellectual property, *i.e.* trademarks. The district court reasoned, however, that although the Lanham Act itself deals with intellectual property, Enigma's false advertising

claim did not relate to any type of intellectual property and therefore § 230 immunity encompassed that claim as well. Having concluded that Malwarebytes was immune on all four claims, the district court dismissed the complaint and granted judgment for Malwarebytes.

On appeal, Enigma primarily contends that the district court erred in interpreting our *Zango* opinion to give online service providers unlimited discretion to block online content, and that the Good Samaritan blocking provision does not provide such sweeping immunity that it encompasses anticompetitive conduct.

## ***DISCUSSION***

### **I. Scope of § 230(c)(2) Immunity as Applied to State-Law Claims**

The district court held that our opinion in *Zango* controlled, and interpreted *Zango* to mean that an online-service provider cannot be liable for blocking internet users from accessing online content that the provider considers objectionable, regardless of the provider's motivations or the harmful effects of the blocking. The scope of the statutory catchall phrase, "otherwise objectionable," was not at issue in *Zango*, however. The central issue in *Zango* was whether § 230 immunity applies to filtering software providers like the defendant Kaspersky in that case, and both parties in this case. *See* 568 F.3d at 1173, 1176. We held such providers had immunity. *Id.* at 1177-78. At the end of our majority opinion, we emphasized the relevant statutory language in stating that § 230 permits providers to block material "that either the provider *or* the user



considers . . . objectionable.” *See id.* at 1177 (original emphasis). The district court focused on that sentence and reasoned that Malwarebytes had unfettered discretion to select what criteria makes a program “objectionable” under § 230, and further, that the court was not to analyze Malwarebytes’s reasons for doing so.

The majority in *Zango* did not, however, address whether there were limitations on a provider’s discretion to declare online content “objectionable.” No such issue was raised in the appeal. We noted that *Zango* “waived” the argument that its software was not “objectionable.” *See id.* at 1176-77. We therefore held that § 230 immunity covered Kaspersky’s decision to block users from accessing the type of content at issue in that case and concluded that § 230 permits providers to block material that “the provider considers . . . objectionable.” *Id.* at 1177.

It was Judge Fisher’s concurring opinion in *Zango* that framed the issue for future litigation as to whether the term “objectionable” might be construed in a way that would immunize providers even if they blocked online content for improper reasons. *See id.* at 1178-80 (Fisher, J. concurring). Judge Fisher warned that extending immunity beyond the facts of that case could “pose serious problems,” particularly where a provider is charged with using § 230 immunity to advance an anticompetitive agenda. *See id.* at 1178. He said that an “unbounded” reading of the phrase “otherwise objectionable” would allow a content provider to “block content for anticompetitive purposes or merely at its malicious whim.” *Id.*

District courts nationwide have grappled with the issues discussed in *Zango*'s majority and concurring opinions, and have reached differing results. Like the district court in this case, at least two other federal district courts have relied on *Zango* to dismiss software-provider lawsuits against Malwarebytes where the plaintiff claimed that Malwarebytes improperly characterized the plaintiffs software as a PUP. See *PC Drivers Headquarters, LP v. Malwarebytes Inc.*, 371 F. Supp. 3d 652 (N.D. Cal. 2019); *PC Drivers Headquarters, LP v. Malwarebytes, Inc.*, No. 1:18-CV-234-RP, 2018 WL 2996897, at \*1 (W.D. Tex. Apr. 23, 2018).

Other district courts have viewed our holding in *Zango* to be less expansive. See *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 884 (N.D. Cal. 2015) (noting that just because “the statute requires the user or service provider to subjectively believe the blocked or screened material is objectionable does not mean anything or everything YouTube finds subjectively objectionable is within the scope of Section 230(c),” and concluding that, “[o]n the contrary such an ‘unbounded’ reading . . . would enable content providers to ‘block content for anticompetitive reasons[.]’”) (quoting Judge Fisher’s concurrence in *Zango*); *Sherman v. Yahoo! Inc.*, 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014) (same); see also *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. Mar. 11, 2011) (acknowledging that a provider’s subjective determination of what constitutes objectionable material under § 230(c)(2) is not limitless, but finding that the harassing emails in that case were reasonably objectionable).

We find these decisions recognizing limitations in the scope of immunity to be persuasive. The courts interpreting *Zango* as providing unlimited immunity seem to us to have stretched our opinion in *Zango* too far. This is because the focus of that appeal was neither what type of material may be blocked, nor why it may be blocked, but rather who benefits from § 230 immunity. The issue was whether § 230 immunity applies to filtering-software providers. *See Zango*, 568 F.3d at 1173. We answered that question in the affirmative, explaining that Kaspersky was the type of “interactive computer service” to which § 230(c)(2) expressly referred, and that Kaspersky was engaged in the type of conduct to which § 230(c)(2) generally applies. *Id.* at 1175-76.

As relevant here, the majority opinion in *Zango* establishes only that Malwarebytes, as a filtering-software provider, is an entity to which the immunity afforded by § 230 would apply. The majority opinion does not require us to hold that we lack the authority to question Malwarebytes’s determinations of what content to block. We must therefore in this case analyze § 230 to decide what limitations, if any, there are on the ability of a filtering software provider to block users from receiving online programming.

The legal question before us is whether § 230(c)(2) immunizes blocking and filtering decisions that are driven by anticompetitive animus. The majority in *Zango* had no occasion to address the issue, and the parties in that case were not competitors. *See* 568 F. 3d at 1170 (explaining Kaspersky is a security software provider; *Zango* provides an online service for users to stream movies, video games, and music).

This is the first § 230 case we are aware of that involves direct competitors.

In this appeal, Enigma alleges that Malwarebytes blocked Enigma's programs for anticompetitive reasons, not because the programs' content was objectionable within the meaning of § 230, and that § 230 does not provide immunity for anticompetitive conduct. Malwarebytes's position is that, given the catchall, Malwarebytes has immunity regardless of any anticompetitive motives.

We cannot accept Malwarebytes's position, as it appears contrary to CDA's history and purpose. Congress expressly provided that the CDA aims "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services" and to "remove disincentives for the development and utilization of blocking and filtering technologies." § 230(b)(2)–(3). Congress said it gave providers discretion to identify objectionable content in large part to protect competition, not suppress it. *Id.* In other words, Congress wanted to encourage the development of filtration technologies, not to enable software developers to drive each other out of business.

In the infancy of the internet, the unwillingness of Congress to spell out the meaning of "otherwise objectionable" was understandable. The broad grant of protective control over online content may have been more readily acceptable in an era before the potential magnitude of internet communication was fully comprehended. Indeed, the fears of harmful content at the time led Congress to enact, in the same statute, an outright ban on the dissemination

of online pornography, a ban which the Supreme Court swiftly rejected as unconstitutional a year later. *See Reno v. ACLU*, 521 U.S. at 877-79 (striking down 47 U.S.C. § 223).

We must today recognize that interpreting the statute to give providers unbridled discretion to block online content would, as Judge Fisher warned, enable and potentially motivate internet-service providers to act for their own, and not the public, benefit. *See* 568 F.3d at 1178 (Fisher, J., concurring). Immunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy. *See* § 230(b)(3) (to maximize user control over what content they view). Indeed, users selecting a security software provider must trust that the provider will block material consistent with that user's desires. Users would not reasonably anticipate providers blocking valuable online content in order to stifle competition. Immunizing anticompetitive blocking would, therefore, be contrary to another of the statute's express policies: "removing disincentives for the utilization of blocking and filtering technologies." *Id.* § 230(b)(4).

We therefore reject Malwarebytes's position that § 230 immunity applies regardless of anticompetitive purpose. But we cannot, as Enigma asks us to do, ignore the breadth of the term "objectionable" by construing it to cover only material that is sexual or violent in nature. Enigma would have us read the general, catchall phrase "otherwise objectionable" as limited to the categories of online material described in the seven specific categories that precede it. *See* 47

U.S.C. § 230(c)(2) (describing material that is “obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable.”). Enigma argues that its software has no such content, and that Malwarebytes therefore cannot claim immunity for blocking it.

Enigma relies on the principle of *ejusdem generis*, which teaches that when a generic term follows specific terms, the generic term should be construed to reference subjects akin to those with the specific enumeration. *See, e.g., Norfolk & W. Ry. Co. v. Am. Train Dispatchers Ass’n*, 499 U.S. 117, 129 (1991). But the specific categories listed in § 230(c)(2) vary greatly: Material that is lewd or lascivious is not necessarily similar to material that is violent, or material that is harassing. If the enumerated categories are not similar, they provide little or no assistance in interpreting the more general category. We have previously recognized this concept. *See Sacramento Reg’l Cty. Sanitation Dist. v. Reilly*, 905 F.2d 1262, 1270 (9th Cir. 1990) (“Where the list of objects that precedes the ‘or other’ phrase is dissimilar, *ejusdem generis* does not apply”).

We think that the catchall was more likely intended to encapsulate forms of unwanted online content that Congress could not identify in the 1990s. But even if *ejusdem generis* did apply, it would not support Enigma’s narrow interpretation of “otherwise objectionable.” Congress wanted to give internet users tools to avoid not only violent or sexually explicit materials, but also harassing materials. Spam, malware and adware could fairly be placed close enough to harassing materials to at least be called “otherwise objectionable” while still

being faithful to the principle of *ejusdem generis*. Several district courts have, for example, regarded unsolicited marketing emails as “objectionable.” See, e.g., *Holomaxx*, 783 F. Supp. 2d at 1104; *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 608-610 (N.D. Ill. 2008); see also *Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, No. CIV09-4567-RBK-KMW, 2010 WL 1799456, at \*6 (D.N.J. May 4, 2010). But we do not, in this appeal, determine the precise relationship between the term “otherwise objectionable” and the seven categories that precede it. We conclude only that if a provider’s basis for objecting to and seeking to block materials is because those materials benefit a competitor, the objection would not fall within any category listed in the statute and the immunity would not apply.

Malwarebytes’s fallback position is that, even if it would lack immunity for anticompetitive blocking, Malwarebytes has found Enigma’s programs “objectionable” for legitimate reasons based on the programs’ content. Malwarebytes asserts that Enigma’s programs, SpyHunter and RegHunter, use “deceptive tactics” to scare users into believing that they have to download Enigma’s programs to prevent their computers from being infected. Enigma alleges, however, that its programs “pose no security threat” and that Malwarebytes’s justification for blocking these “legitimate” and “highly regarded” programs was a guise for anticompetitive animus.

The district court interpreted our holding in *Zango* to foreclose this debate entirely, implicitly reasoning that if Malwarebytes has sole discretion to select what programs are “objectionable,” the court need not evaluate the reasons for the designation. Because

we hold that § 230 does not provide immunity for blocking a competitor's program for anticompetitive reasons, and because Enigma has specifically alleged that the blocking here was anticompetitive, Enigma's claims survive the motion to dismiss. We therefore reverse the dismissal of Enigma's state-law claims and we remand for further proceedings.

## **II. The Federal Claim and the CDA's Intellectual Property Exception**

Enigma's fourth claim is a claim for false advertising under the Lanham Act, a statute dealing with a form of intellectual property, *i.e.* trademarks. Enigma alleges that Malwarebytes publicly mischaracterized Enigma's programs SpyHunter and RegHunter as potentially unwanted or PUPs, and it did so in order to interfere with Enigma's customer base and divert those customers to Malwarebytes.

Section 230(e)(2) of the CDA contains an exception to immunity for intellectual property claims. *See* 47 U.S.C. § 230(e)(2). This exception, known as the intellectual property carve out, states that § 230 immunity shall not "limit or expand any law pertaining to intellectual property." *Id.* In light of that exception, Enigma contends that immunity would not bar Enigma's Lanham Act claim, even if immunity is available to Malwarebytes on the state law claims. Although Enigma's claim does not itself involve an intellectual property right, Enigma characterizes its federal false advertising claim as one "pertaining to intellectual property" within the meaning of § 230(e)(2) because the Lanham Act deals with intellectual property. The district court rejected this argument, and rightly so.



This is because even though the Lanham Act is known as the federal trademark statute, not all claims brought under the statute involve trademarks. The Act contains two parts, one governing trademark infringement and another governing false designations of origin, false descriptions, and dilution. *Compare* 15 U.S.C. § 1114 (trademark infringement) *with id.* § 1125 (the rest). The latter, § 1125, creates two bases of liability, false association and false advertising. *Compare* § 1125 (a)(1)(A) (false association) *with* § 1125 (a)(1)(B) (false advertising). Thus, although “much of the Lanham Act addresses the registration, use, and infringement of trademarks and related marks, . . . § 1125(a) is one of the few provisions that goes beyond trademark protection.” *Dastar Corp. v. Twentieth Cent. Fox Film Corp.*, 539 U.S. 23, 28-29 (2003).

In this appeal, we must decide whether the exception to immunity contained in § 230(e)(2) applies to false advertising claims brought under the Lanham Act. Our court has not addressed the issue, although we have considered the exception as it would apply to state law claims. *See Perfect 10 v. CCBill, LLC*, 488 F.3d 1102, 1118-19 (9th Cir. 2009) (concluding that the intellectual property exception in § 230(e)(2) was not intended to cover intellectual property claims brought under state law); *see also Gen. Steel Domestic Sales, L.L.C. v. Chumley*, 840 F.3d 1178, 1182 (10th Cir. 2016) (declining to analyze the intellectual property exception; explaining that because “§ 230 does not contain the grant of immunity from suit contended for, it is unnecessary to discuss its applicability to the Lanham Act false advertising claims”).

We have observed before that because Congress did not define the term “intellectual property law,” it should be construed narrowly to advance the CDA’s express policy of providing broad immunity. *See Perfect 10*, 488 F.3d at 1119. One of these express policy reasons for providing immunity was, as Congress stated in § 230(b)(2), “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). The intellectual property exception is a limitation on immunity, and the CDA’s stated congressional purpose counsels against an expansive interpretation of the exception that would diminish the scope of immunity. If the intellectual property law exception were to encompass any claim raised under the Lanham Act—including false advertising claims that do not directly involve intellectual property rights—it would create a potential for new liability that would upset, rather than “preserve” the vibrant culture of innovation on the internet that Congress envisioned. *Id.*

We therefore hold that the intellectual property exception contained in § 230(e)(2) encompasses claims pertaining to an established intellectual property right under federal law, like those inherent in a patent, copyright, or trademark. The exception does not apply to false advertising claims brought under § 1125(a) of the Lanham Act, unless the claim itself involves intellectual property.

Here, Enigma’s Lanham Act claim derives from the statute’s false advertising provision. Enigma alleges that Malwarebytes mischaracterized Enigma’s most popular software programs in order to divert

Enigma's customers to Malwarebytes. These allegations do not relate to or involve trademark rights or any other intellectual property rights. Thus, Enigma's false advertising claim is not a claim "pertaining to intellectual property law" within the meaning of § 230(e)(2). The district court correctly concluded that the intellectual property exception to immunity does not encompass Enigma's Lanham Act claim.

The district court went on to hold, however, as it did with the state law claims, that Malwarebytes is nevertheless immune from liability under our decision in *Zango*. As we have explained with respect to the state law claims, *Zango* did not define an unlimited scope of immunity under § 230, and immunity under that section does not extend to anticompetitive conduct. Because the federal claim, like the state claims, is based on allegations of such conduct, the federal claim survives dismissal. We therefore reverse the district court's judgment in favor of Malwarebytes and remand for further proceedings on this claim as well.

### ***CONCLUSION***

The judgment of the district court is reversed and the case is remanded for further proceedings consistent with this opinion.

**REVERSED and REMANDED.**

---

RAWLINSON, Circuit Judge, dissenting:

In his concurring opinion in *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1179-80 (9th Cir. 2009), Judge Fisher acknowledged that “until Congress clarifies the statute or a future litigant makes the case for a possible limitation,” the “broadly worded” Communications Decency Act (the Act) afforded immunity to a distributor of Internet security software. Congress has not further clarified the statute and Enigma Software has not persuasively made a case for limitation of the statute beyond its provisions.

The majority opinion seeks to limit the statute based on the fact that the parties are competitors. *See Majority Opinion*, p. 4. However, nothing in the statutory provisions or our majority opinion in *Zango* supports such a distinction. Rather the “broad language” of the Act specifically encompasses “any action voluntarily taken [by a provider] to restrict access to . . . material that the provider . . . considers to be . . . otherwise objectionable.” 47 U.S.C. § 230(c)(2)(A) (emphasis added). Under the language of the Act, so long as the provider’s action is taken to remove “otherwise objectionable” material, the restriction of access is immunized. *See id.* The majority’s real complaint is not that the district court construed the statute too broadly, but that the statute is written too broadly. However, that defect, if it is a defect, is one beyond our authority to correct. *See Baker Botts LLP v. ASARCO LLC*, 135 S. Ct. 2158, 2169 (2015).

In particular, the majority holds that the criteria for blocking online material may not be based on the

identity of the entity that produced it. *See Majority Opinion*, p. 10. Unfortunately, however, that conclusion cannot be squared with the broad language of the Act. Under the language of the statute, if the blocked content is “otherwise objectionable” to the provider, the Act bestows immunity. *Zango*, 568 F.3d at 1173 (“[T]he statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user *or the provider* deems objectionable.”) (emphasis in the original); 1174 (“According protection to providers of programs that filter adware and malware is also consistent with the Congressional goals for immunity articulated in [47 U.S.C.] § 230 itself.”). Although the parties were not direct competitors, the plaintiff in *Zango* asserted similar anti-competition effects. *See id.* at 1171-72. The majority’s policy arguments are in conflict with our recognition in *Zango* that the broad language of the Act is consistent with “the Congressional goals for immunity” as expressed in the language of the statute. *Id.* at 1174. As the district court cogently noted, we “must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Connecticut Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (citations omitted).

I respectfully dissent.

57a

**APPENDIX C**

---

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

---

ENIGMA SOFTWARE GROUP USA LLC,

*Plaintiff,*

v.

MALWAREBYTES INC.,

*Defendant.*

---

Case No. 5:17-cv-02915-EJD

---

Filed: November 7, 2017

---

**ORDER GRANTING DEFENDANT'S MOTION  
TO DISMISS**

Re: Dkt. No. 97

---

Plaintiff Enigma Software Group USA LLC (“Enigma”) brings claims against Defendant Malwarebytes Inc. based on its allegation that Malwarebytes unlawfully characterized Enigma’s software as harmful to users’ computers. Malwarebytes now moves to dismiss under Fed. R. Civ. P. 12(b)(6). Malwarebytes’s motion will be granted.

## I. BACKGROUND

Malwarebytes develops software that protects internet users from malware, adware, and other unwanted computer programs. First Am. Compl. (“FAC”) ¶¶ 3, 36, Dkt. No. 33. Malwarebytes’s software scans users’ computers for “potentially unwanted programs,” which it automatically flags and quarantines. *Id.* ¶ 5. When the software detects an unwanted program, it displays a notification and asks the user if she wants to remove the program from her computer. *Id.*

Enigma also provides anti-malware software to internet users. *Id.* ¶ 4. Enigma alleges that, in 2016, Malwarebytes revised the criteria it uses to identify unwanted programs. *Id.* ¶ 7. Under the new criteria, Malwarebytes’s software identifies Enigma’s software as a potential threat. *Id.* Enigma alleges that Malwarebytes’s classification of Enigma’s software is wrong because Enigma’s programs “are legitimate and pose no security threat to users’ computers.” *Id.* ¶ 9. Enigma alleges that Malwarebytes revised its criteria to interfere with Enigma’s customer base and to retaliate against Enigma for a separate lawsuit Enigma filed against a Malwarebytes affiliate. *Id.* ¶¶ 8, 19–20.

On that basis, Enigma brings claims for (1) false advertising in violation of § 43(a) of the Lanham Act (FAC ¶¶ 134–43), (2) violations of New York General Business Law § 349<sup>1</sup> (FAC ¶¶ 144–50), (3) tortious interference with contractual relations (FAC ¶¶ 151–

---

<sup>1</sup> This case was transferred from the Southern District of New York on May 12, 2017. Dkt. No. 67.

160), and (4) tortious interference with business relations (FAC §§ 161–68).

Malwarebytes now moves to dismiss under Fed. R. Civ. P. 12(b)(6). Def.’s Mot. to Dismiss (“MTD”), Dkt. No. 97.

## II. LEGAL STANDARD

A motion to dismiss under Fed. R. Civ. P. 12(b)(6) tests the legal sufficiency of claims alleged in the complaint. Parks Sch. of Bus., Inc. v. Symington, 51 F.3d 1480, 1484 (9th Cir. 1995). Dismissal “is proper only where there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory.” Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). The complaint “must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’ ” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

## III. DISCUSSION

Malwarebytes argues that all of Enigma’s claims are barred by the immunity provisions of § 230(c)(2) of the Communications Decency Act. Mot. 7. That section provides:

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise



objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

47 U.S.C. § 230(c)(2). Congress enacted these provisions “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 to encourage “development and utilization of blocking and filtering technologies.” *Id.* § 230(b)(3), (4).

Malwarebytes argues that this case is “indistinguishable” from the Ninth Circuit’s opinion in *Zango* interpreting § 230(c)(2). Mot. 8; *Zango, Inc. v. Kaspersky*, 568 F.3d 1169 (9th Cir. 2009). In that case, Zango alleged that Kaspersky’s anti-malware software incorrectly classified Zango’s software as harmful. *Zango*, 568 F.3d at 1170–71. The Ninth Circuit considered whether “companies that provide filtering tools,” such as Kaspersky, are eligible for immunity under § 230(c). *Id.* at 1173. The panel first explained that providers of blocking software are eligible for § 230(c)(2) immunity as long as they meet the statutory requirements. *Id.* at 1173–75. Next, it found that Kaspersky was an “interactive computer service” within the meaning of the statute. *Id.* at 1175–76. It also found that Kaspersky “has ‘made available’ for its users the technical means to restrict items that Kaspersky has defined as malware.” *Id.* at 1176. The panel found that Kaspersky qualified for

immunity under § 230(c)(2)(B) “so long as the blocked items are objectionable material under § 230(c)(2)(A).” *Id.* It concluded that Kaspersky properly classified malware as “objectionable” material, and as such, it found that Kaspersky satisfied the requirements for immunity under § 230(c)(2)(B). *Id.* at 1177–78 (holding that any “provider of access tools that filter, screen, allow, or disallow content that the provider or user considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable is protected from liability by 47 U.S.C. § 230(c)(2)(B) for any action taken to make available to others the technical means to restrict access to that material”).

Enigma argues that Zango is distinguishable in two respects. First, Enigma argues that malware, as defined by Malwarebytes’s criteria, is not one of the types of materials to which § 230(c)(2) immunity applies. Pl.’s Opp’n to Def.’s Mot. to Dismiss (“Opp’n”) 11–12, 14, Dkt. No. 100. By its terms, § 230(c)(2)(A) applies to material that is “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” § 230(c)(2)(B) applies to the same material.<sup>2</sup> Enigma argues that malware is not within the scope of “objectionable” material because it is “not remotely related to the content categories enumerated” in subsection (A) (i.e., materials that are “obscene, lewd, lascivious,” and so on). Opp’n 10. Enigma further argues that

---

<sup>2</sup> Subsection (B) refers to “material described in paragraph (1).” This is a typo in the statute; it should read: “material described in paragraph (A).” See Zango, 568 F.3d at 1173 n.5 (“‘paragraph (1)’ is a scrivener’s error referring to ‘paragraph (A)’”).

Zango did not address whether an anti-malware provider has discretion to decide what is “objectionable,” because, as the Ninth Circuit noted, Zango waived that argument by failing to raise it in its opening appellate brief. Id.; Zango, 568 F.3d at 1175–76.

However, while it is true that the Zango panel found that Zango waived this argument, Enigma overlooks Zango’s clear holding that § 230(c)(2)(B) immunity applies to “a provider of computer services that makes available software that filters or screens material that the user or the provider deems objectionable.” Zango, 568 F.3d at 1173 (emphasis in original); see also id. at 1177 (holding that immunity applies to material “that the provider or user considers . . . objectionable”) (emphasis added); id. (immunity applies to “material that either the user or the provider deems objectionable”) (emphasis in original). This interpretation of Zango aligns with the plain language of the statute, which likewise states that immunity applies to “material that the provider or user considers to be . . . objectionable.” 47 U.S.C. § 230(c)(2)(A) (emphasis added). In Zango, the provider of the anti-malware software, Kaspersky, exercised its discretion to select the criteria it would use to identify objectionable computer programs. The Ninth Circuit held that malware, as Kaspersky defined it, was properly within the scope of “objectionable” material. In that respect, the Court agrees with Malwarebytes that Zango is factually indistinguishable from the scenario here.

Second, Enigma argues that Malwarebytes is entitled to § 230(c)(2)(B) immunity only if it acted in “good faith.” Opp’n 11–14. Subsection (A) protects

“any action voluntarily taken in good faith” to restrict access to objectionable material (emphasis added). Subsection (B) does not contain a good-faith requirement. Nonetheless, Enigma argues that good faith is “an implied requirement in subsection (B) that is part and parcel of the proper, plain meaning of the statute when read as a whole.” Opp’n 14. The Zango court did not decide whether subsection (B) contains a good-faith requirement, since Zango waived that argument on appeal and the panel did not need to resolve it to reach its decision. Zango, 568 F.3d at 1177. However, as the panel recognized, subsection (B) “has no good faith language.” Id. Here, the Court must assume that Congress acted intentionally when it decided to include a good-faith requirement in subsection (A) but not in (B). See, e.g., Conn. Nat’l Bank v. Germain, 503 U.S. 249, 253–54 (1992) (“[I]n interpreting a statute a court should always turn first to one, cardinal canon before all others. We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.”); Bailey v. United States, 516 U.S. 137, 146 (1995) (“The difference between the two provisions demonstrates that, had Congress meant to broaden application of the statute . . . , Congress could and would have so specified.”). This reading is bolstered by the fact that subsection (B) includes an explicit reference to subsection (A) with respect to the types of material to which immunity applies. Congress could have included a similar reference in subsection (B) to subsection (A)’s good-faith requirement, but it chose not to. As such, the Court agrees with Malwarebytes that it need not consider whether Malwarebytes acted in good faith for the purposes of

deciding whether Malwarebytes is entitled to immunity under § 230(c)(2)(B). Def.'s Reply in Support of Mot. to Dismiss ("Reply") 5–7, Dkt. No. 102.

Enigma argues Malwarebytes is nonetheless ineligible for immunity with respect to Enigma's Lanham Act claim (FAC ¶¶ 134–143) because § 230 provides that "nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2); Opp'n 15.<sup>3</sup> Enigma's argument fails because its complaint does not allege an intellectual property claim. The Lanham Act contains two parts: one governing trademark infringement (15 U.S.C. § 1114) and one governing unfair competition (15 U.S.C. § 1125(a)). The unfair competition provision, in turn, "creates two distinct bases of liability": one governing false association (15 U.S.C. § 1125(a)(1)(A)) and one governing false advertising (15 U.S.C. § 1125(a)(1)(B)). Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1384 (2014). Enigma's complaint asserts a false advertising claim under § 1125(a)(1)(B). FAC ¶ 135. Enigma does not assert claims under the trademark provisions of the Lanham Act. The complaint does not allege that Enigma owns trademarks or any other form of intellectual property, nor does it allege that Malwarebytes has committed any form of intellectual property infringement, including misuse of its trademarks. Accordingly, the Court finds that Enigma's false

---

<sup>3</sup> Enigma does not dispute that immunity would apply to its other three claims for business torts. Opp'n 15; see also Zango, 568 F.3d at 1177 ("we have interpreted § 230 immunity to cover business torts").

advertising claim under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), does not arise under a “law pertaining to intellectual property” under 47 U.S.C. § 230(e)(2). See Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1109–10 (C.D. Cal. 2004) (“Since false advertising . . . does not pertain to intellectual property rights, the Court finds that the immunity provided under the CDA for [the plaintiff’s] false advertising claim is not excluded under § 230(e)(2).”).

#### **IV. CONCLUSION**

Because Malwarebytes is entitled to immunity under 47 U.S.C. § 230(c)(2)(B) with respect to all of Enigma’s claims, Malwarebytes’s motion to dismiss is GRANTED. The Clerk shall close this file.

#### **IT IS SO ORDERED.**

Dated: November 7, 2017

/s/  
EDWARD J. DAVILA  
United States District Judge

**APPENDIX D**

---

**STATUTORY PROVISIONS INVOLVED**

---

**1. 47 U.S.C. § 230 provides:**

**Protection for private blocking and screening  
of offensive material**

**(a) Findings**

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These 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.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

**(b) Policy**

It is the policy of the United States—

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) 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;

(3) 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;

(4) 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; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

**(c) Protection for “Good Samaritan” blocking and screening of offensive material**

**(1) Treatment of publisher or speaker**

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.



**(2) Civil liability**

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).<sup>1</sup>

**(d) Obligations of interactive computer service**

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

**(e) Effect on other laws**

**(1) No effect on criminal law**

---

<sup>1</sup> So in original. Probably should be “subparagraph (A).”

69a

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

**(2) No effect on intellectual property law**

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

**(3) State law**

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

**(4) No effect on communications privacy law**

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

**(5) No effect on sex trafficking law**

Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

(A) any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the

70a

charge would constitute a violation of section 1591 of title 18; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

**(f) Definitions**

As used in this section:

**(1) Internet**

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

**(2) Interactive computer service**

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

**(3) Information content provider**

The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

**(4) Access software provider**

The term “access software provider” means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

2. **47 U.S.C. § 230 (2012) provides:**

**Protection for private blocking and screening  
of offensive material**

**a) Findings**

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These 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.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

**(b) Policy**

It is the policy of the United States—

### 73a

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) 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;

(3) 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;

(4) 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; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

#### **(c) Protection for "Good Samaritan" blocking and screening of offensive material**

##### **(1) Treatment of publisher or speaker**

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

##### **(2) Civil liability**

74a

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).<sup>1</sup>

**(d) Obligations of interactive computer service**

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

**(e) Effect on other laws**

**(1) No effect on criminal law**

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of

---

<sup>1</sup> So in original. Probably should be “subparagraph (A).”

this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

**(2) No effect on intellectual property law**

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

**(3) State law**

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

**(4) No effect on communications privacy law**

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

**(f) Definitions**

As used in this section:

**(1) Internet**

The term “Internet” means the international computer network of both Federal and non-Federal interoperable packet switched data networks.



**(2) Interactive computer service**

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

**(3) Information content provider**

The term “information content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

**(4) Access software provider**

The term “access software provider” means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

- (A) filter, screen, allow, or disallow content;
- (B) pick, choose, analyze, or digest content; or
- (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.