No. 17-17351

IN THE

United States Court of Appeals for the Ninth Circuit

ENIGMA SOFTWARE GROUP USA, LLC,

Plaintiff-Appellant,

v.

MALWAREBYTES, INC.,

Defendant-Appellee.

On Appeal from the United States District Court
for the Northern District of California, No. 5:17-cv-02915-EJD
District Judge Edward J. Davila

PETITION FOR PANEL REHEARING AND REHEARING EN BANC

TYLER GRIFFIN NEWBY
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Fax: (415) 281-1350
Email: tnewby@fenwick.com

NEAL KUMAR KATYAL
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, DC 20004
Telephone: (202) 637-5600
Fax: (202) 637-5910
Email: neal.katyal@hoganlovells.com

Attorneys for Defendant-Appellee Malwarebytes, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES:

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

RULE 35(b) STATEMENT

When the Internet was a new technology, Congress adopted a novel approach to keeping users safe from its many emerging threats. Rather than embroil regulators in the near-impossible task of serving as the Internet's police officers, Congress encouraged Internet users to protect themselves using technology to filter and disable those threats. To spur development of such technology, in Section 230(c)(2)(B) of the Communications Decency Act of 1996 ("CDA"), Congress immunized from suit providers of "the technical means to restrict access" to "material that the provider or user considers," among other things, "objectionable." Control therefore was given to Internet users, who could choose whatever filtering technology suited their needs without the interference of courts. For over twenty years, that immunity has stimulated a "vibrant and competitive free market" for filtering software. 47 U.S.C. § 230(b)(2). This Court first recognized that immunity—and its value—in *Zango, Inc.* v. *Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173-74 (9th Cir. 2009).

The divided panel opinion in this case strikes at the heart of the system Congress created. Bypassing familiar rules of statutory construction and this Court's opinion in *Zango*, the majority effectively rewrote Section 230 in light of its own (misguided) understanding of the policy interests at stake. Specifically, the majority held that the statute contains an unstated exception to immunity allowing

a lawsuit any time a plaintiff can plausibly allege that the defendant's filtering technology has some "anticompetitive" motivation.

That exception threatens to swallow the rule. Because malicious software can easily masquerade as legitimate, its developers can seek to avoid being filtered by filing retaliatory lawsuits that will now survive until at least summary judgment. And by blessing an atextual exception for "anticompetitive" filtering, the panel has opened the open for courts in this Circuit—which covers the epicenter of technological development—to fashion further exceptions inviting additional litigation. Such lawsuits will impose substantial costs on bona fide security firms, making those firms more cautious in developing filtering tools and deterring the development of cutting-edge technology capable of combatting the latest threats. Users will have fewer choices and be less safe as a result.

Worse still, the exception is unnecessary to address the majority's policy concerns. The majority worried that software developers would use immunity as cover to "stifle competition" by blocking competitors. Add. 18. But Congress anticipated this problem. Elsewhere in the statute, it provided that the immunity for entities that actually "restrict access" to content applies only for actions "voluntarily taken in good faith." 47 U.S.C. § 230(c)(2)(A). By contrast, an entity—like Malwarebytes—that provides *others* the "technical means" to filter content poses no similar threat. Such software leaves users in the driver seat.

Thus, Congress omitted the good faith requirement from Section 230(c)(2)(B)'s immunity for providers of filtering technology. Giving effect to the text Congress enacted would therefore fully address the majority's concerns about "anticompetitive blocking." Add. 18.

Instead, the majority overlooked these crucial differences and swapped user control for regulation by courts. That is not the system that Congress enacted or intended. Indeed, the majority's opinion is already provoking disagreement: Just last week, the California Superior Court issued a tentative ruling "disagree[ing]" with the panel's approach, finding that it "ignore[s] the plain language of the statute." *Prager Univ.* v. *Google LLC*, No. 19-CV-340667 (Cal. Super. Ct. Santa Clara Cty. Oct. 25, 2019) (tentative ruling), Add. 39. Rehearing is necessary to realign this Court's reading of Section 230 with Congress's text and this Court's precedent and stave off further conflict with state courts in this Circuit.

BACKGROUND

1. The CDA emerged in 1996 as a response to the proliferation of offensive content on the nascent Internet. 141 Cong. Rec. 22,044-45 (1995) (statement of Rep. Cox). The Senate originally proposed a somewhat blunt instrument for combatting the problem: imposing "civil and criminal penalties" directly on peddlers of "offensive material." *Force* v. *Facebook, Inc.*, 934 F.3d 53, 78 (2d Cir. 2019) (Katzmann, C.J., concurring in part) (citing 141 Cong. Rec. 15,505 (1995)).

The House recognized that this approach was unrealistic. Because "there is just too much going on on the Internet," direct government regulation would prove ineffective "[n]o matter how big the army of bureaucrats." 141 Cong. Rec. 22,045 (statement of Rep. Cox). The House therefore proposed a more innovative approach that would let "Government * * * get out of the way and let parents and individuals" "tailor what [they] see to [their] own tastes." *Id.*

The House provision, which ultimately became Section 230, takes a two-pronged approach. The first prong addresses a "provider or user of an interactive computer service" that directly "restrict[s] 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). It immunizes such providers from suit for "any action voluntarily taken in good faith." *Id.* The second prong—at issue here—addresses immunity for a different type of "provider or user": one who acts "to enable or make available to information content providers or others the technical means to restrict access to [the] material described in [sub]paragraph [A]."[1] *Id.* § 230(c)(2)(B). For those providing the "technical means" to filter content, the statute offers immunity for "any action," without reference to "good faith."

[1] The text as enacted reads "material described in paragraph (1)," but that is a typo. *Zango*, 568 F.3d at 1173 n.5.

Congress also included in the CDA's text multiple competing policy goals. Three are relevant to this case: (1) encouraging "the development of technologies which maximize user control over what information is received," 47 U.S.C. § 230(b)(3); (2) removing "disincentives for the development and utilization of blocking and filtering technologies," *id.* § 230(b)(4); and (3) preserving "the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation," *id.* § 230(b)(2).

2. Malwarebytes, Inc. is a leading Internet security firm. Add. 10. Users download its software to protect themselves from a wide array of threats on the Internet, including "malware," which can damage operating systems or steal user information, and "potentially unwanted programs" (or "PUPs") that deceive users into thinking something is wrong with their computer so that they will download premium, paid products to combat the supposed threats. When Malwarebytes's software detects a threat, it disables the program, notifies the user, and offers the option to retain, quarantine, or remove the offending material. *See* Excerpts of Record ("ER") 39-46. In other words, *users* make the final decision about what gets filtered.

In October 2016, employing its experience and judgment, Malwarebytes adopted new criteria for what it considers a PUP. ER 38. Using those criteria,

Malwarebytes's software began classifying certain products of plaintiff Enigma Software Group as PUPs. Add. 11. As with any PUP, Malwarebytes's software gave users the option to retain or remove Enigma's programs, although Enigma alleges that some users might find retaining the programs technically challenging. *See* ER 39-46.

Enigma sued Malwarebytes, alleging state-law business torts and unfair advertising in violation of the Lanham Act. ER 55-60. Malwarebytes moved to dismiss, invoking Section 230(c)(2)(B)'s immunity for providers of filtering software. Add. 12. Enigma opposed the motion, claiming that Malwarebytes's PUP criteria revision was part of an "anti-competitive, predatory scheme to deliberately injure" Enigma and that immunity is unavailable under such circumstances. ER 27.

The District Court agreed with Malwarebytes, concluding that this case was "factually indistinguishable" from the situation this Court confronted in *Zango*. ER 6. In that case, another Internet security firm had been sued on a theory similar to Enigma's. *Zango*, 568 F.3d at 1172. This Court held that the security firm was entitled to claim Section 230(c)(2)(B)'s immunity for "a provider of software or enabling tools that filter, screen, allow, or disallow content that the provider or user considers * * * objectionable." *Id.* at 1173. Seeing no material difference between Malwarebytes and the *Zango* defendant, the District Court applied the same

immunity here. The court also rejected Enigma's argument that Section 230(c)(2)(B) immunity requires "good faith." Examining the statute's text, the court emphasized that the adjacent provision—providing immunity for those who actually "restrict access to or availability of material"—included a good faith requirement. ER 4 (quoting 47 U.S.C. § 230(c)(2)(A)). "Congress could have included a similar reference in sub[paragraph] (B)," the District Court explained, "but it chose not to." ER 7. The court therefore held Malwarebytes immune.

A divided panel of this Court reversed. The majority did not read *Zango* to address whether there are "limitations * * * on the ability of a filtering software provider to block users from receiving online programming." Add. 16. And it thought that the "CDA's history and purpose" favored reading an implied limitation into the statute when a firm allegedly acts with "anticompetitive motives." *Id.* at 17. Finding that "Enigma has specifically alleged that the blocking here was anticompetitive," the majority held that the lawsuit cannot be dismissed at this stage.[2] *Id.* at 20.

Judge Rawlinson dissented. "[T]he 'broad language' of the Act," she explained, "bestows immunity" "if the blocked content is 'otherwise objectionable' *to the provider*." *Id.* at 25 (quoting *Zango*, 568 F.3d at 1173). Judge Rawlinson

[2] Separately, the panel held that Enigma's allegation of unfair advertising under the Lanham Act does not fall within the CDA's exception for claims "pertaining to intellectual property." Add. 21 (quoting 47 U.S.C. § 230(e)(2)). Malwarebytes takes no issue with that holding.

also found the majority's narrow approach to immunity to be "in conflict" with this Court's recognition in *Zango* that the "broad language of the Act is consistent with 'the Congressional goals for immunity.'" *Id.* at 25 (quoting *Zango*, 568 F.3d at 1174).

REASONS FOR GRANTING REHEARING

I. THE PANEL'S DECISION CONFLICTS WITH SUPREME COURT AND NINTH CIRCUIT PRECEDENT.

Under standard rules of statutory construction, Malwarebytes is entitled to immunity under Section 230(c)(2)(B). The majority reached a contrary conclusion only by leaving aside the statute's text and undertaking a misguided policymaking exercise. The resulting interpretation cannot be squared with *Zango*'s reading of the statute.

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)); *see also Park 'N Fly, Inc.* v. *Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985) ("Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose."). Only after examining "the text of the provision in question" will the 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). Even then, courts must cautiously wade into policy disputes as they "[l]ack[] the expertise or authority to assess the[] important competing claims" involved in such debates, which are "best addressed to the Congress." *Dunn* v. *CFTC*, 519 U.S. 465, 480 (1997). Thus, this Court has recognized that even when "the statutory language declares" Congress's "goals," courts still "must closely hew to the text of the" "operative section of the" law. *Barnes* v. *Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009), *as amended* (Sept. 28, 2009).

Following those rules here, Malwarebytes's alleged actions fall within Section 230(c)(2)(B)'s protection for providers of filtering technology. That provision immunizes (1) "a provider or user of an interactive computer service" that offers (2) 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). The first element is undisputed; Enigma agrees that Malwarebytes is a "provider of an interactive computer service." *Id.*; *see* ER 23. It is equally obvious that Malwarebytes provides "others" "the technical means to restrict access" to online "material." 47 U.S.C. § 230(c)(2)(B). As Enigma's complaint alleges, Malwarebytes's program works by "detecting * * * malware or other computer threats, reporting to the user the results of the detection, and then

taking remedial action * * * or providing the user with an option to remove the detected program." ER 34.[3]

That leaves only whether Enigma's software is "material" that a "provider" (here, Malwarebytes) or a "user considers to be * * * objectionable." 47 U.S.C. § 230(c)(2)(A). Enigma's own Complaint answers that question in the affirmative, conceding that Malwarebytes "identif[ies]" Enigma's products "as PUPs and 'threats.'" ER 24. That subjective determination is enough. Congress carefully chose its words to enact a subjective test, providing immunity for material that the provider "*considers to be*" objectionable, rather than material that "*is*" objectionable. *Cf. United States* v. *Martin*, 438 F.3d 621, 630 (6th Cir. 2006) (phrase "considers to be" connotes "discretion"). That is exactly how *Zango* read the statute. 568 F.3d at 1173 (immunity covers "material that the user or the provider *deems* objectionable" (emphasis altered)). And the word "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).

[3] Enigma attempted to contest this element before the panel, but "forfeit[ed] * * * [the] issue" by failing to "complain of [it] in the district court." *Loher* v. *Thomas*, 825 F.3d 1103, 1121 (9th Cir. 2016) (internal quotation marks omitted).

Enigma has repeatedly argued that, to qualify for immunity, Malwarebytes must have acted in "good faith"—and, therefore, without anticompetitive animus—when it deemed Enigma's products a PUP. But Section 230(c)(2)(B)'s language contains no such requirement. That choice was plainly intentional: The neighboring provision in subparagraph (A)—which applies to entities that directly "restrict access" to content—immunizes only "action[s] voluntarily taken in good faith." 47 U.S.C. § 230(c)(2)(A). No similarly constraining language appears in Section 230(c)(2)(B). "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); *see also Ariz. Elec. Power Coop., Inc.* v. *United States*, 816 F.2d 1366, 1375 (9th Cir. 1987) (same).

The differential treatment of immunity in subparagraphs (A) and (B) accords with the statute's policy goals. It "encourage[s] the development of technologies that maximize user control," 47 U.S.C. § 230(b)(3), by immunizing providers of such tools—such as Malwarebytes—regardless of motive. *Cf. Zango*, 568 F.3d at 1174 ("[A]ffording the safe harbor to providers of anti-malware software aligns with the Congressional policy" by encouraging "the development of software that filters out objectionable * * * material[.]"). But, to prevent misuse of those tools,

Congress also required those who actually restrict content—for example, a social media site that removes an offensive post—to behave as "Good Samaritans," *id.* § 230(c), by acting in "good faith," *id.* § 230(c)(2)(A).

2. The majority opinion reached a different conclusion by failing to follow the usual order of operations for statutory construction; instead, its analysis began and ended with "the CDA's history and purpose." Add. 17. Relying on those factors, it concluded that Section 230(c)(2)(B) contains an unstated exception for anticompetitive conduct. *Id.* In effect, then, the majority imposed on Section 230(c)(2)(B) the very good-faith requirement that Congress omitted. *See Prager*, Case No. 19-CV-340667, Add. 39 (majority "ignore[d] the plain language of the statute by reading a good faith limitation into section 230(c)(2)(B)"). As Judge Rawlinson explained in dissent, the panel had to disregard the CDA's text to reach that result. Add. 24-25.

The majority never expressly identifies *any* basis in the text for a motive-based exception. It implies, however, that the exception derives from the meaning of "objectionable." *See id.* at 20 ("We conclude only that if a provider's basis for objecting 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."). But the majority made no effort to explain how such a limitation comports with the plain (and broad) meaning of

"objectionable." It cited no definition or precedent construing that word, and, as Judge Rawlinson pointed out, its "conclusion cannot be squared with the broad language of the Act." *Id.* at 25. Stranger still, it found that the only textual argument it considered *favored Malwarebytes*. *Id.* at 18. Enigma had urged the Court to employ the canon of *ejusdem generis* to give "objectionable" a restrictive meaning in light of the six adjectives listed before it. *See id.* at 18-20. The majority rightly recognized that the canon is inappropriate here because "the specific categories listed in § 230(c)(2) vary greatly," and when "enumerated categories are not similar, they provide little or no assistance in interpreting the more general category." *Id.* at 19 (citing *Sacramento Reg'l Cty. Sanitation Dist.* v. *Reilly*, 905 F.2d 1262, 1270 (9th Cir. 1990)).

Finally, despite extensive briefing from both sides on the issue, the majority said nothing about Enigma's argument that subparagraph (A)'s "good faith" requirement should be read as "implied" in subparagraph (B). Enigma Opening Br. 42. Indeed, throughout its analysis, the majority cites the operative provision simply as "Section 230(c)(2)," completely effacing the textual differences between subparagraphs (A) and (B).

Under binding precedent from the Supreme Court and this Circuit, the majority's approach of bypassing the statutory text in favor of pure policy analysis was error. "Policy considerations cannot override * * * interpretation of the text

and structure of the Act[.]" *Cent. Bank of Denver, N.A.* v. *First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 188 (1994). That holds true even where, as here, Congress listed goals in the statutory text: In the context of this very statute, this Court has required "closely hew[ing] to the text of the statutory bar on liability" rather than focusing on the prefatory "goals." *Barnes*, 570 F.3d at 1100. Such policy statements cannot replace the statute's "operative" text. *Id.*; *see also Comcast Corp.* v. *FCC*, 600 F.3d 642, 644 (D.C. Cir. 2010) ("[U]nder Supreme Court * * * case law statements of policy, by themselves, do not create statutorily mandated responsibilities." (internal quotation marks omitted)).

3. Compounding the majority's problems, the panel opinion also conflicts with *Zango*. There, this Court read the CDA to create a subjective test for what is "objectionable," affording immunity so long as the provider or user "*deems*" the filtered material "objectionable." 568 F.3d at 1173 (emphasis added). The majority here scuttles that approach in favor of an objective test, in which a court must determine whether the material is in fact "objectionable" by reference to some external standard. Add. 16. The majority thought it could reconcile the two cases by framing the issue here as whether the statute imposes "limitations * * * on the ability of a filtering software provider" to deem material objectionable. *Id.*; *see*

Zango, 568 F.3d at 1177 n.8. But such limitations must operate within the subjective framework that *Zango* established.[4] The majority's does not.

Moreover, as Judge Rawlinson pointed out, the majority opinion is "in conflict with" *Zango*'s "recognition * * * that the broad language of the Act is consistent with 'the Congressional goals for immunity' as expressed in the language of the statute." Add. 25 (quoting *Zango*, 568 F.3d at 1174). The majority sidesteps that charge by claiming the equities in this case differ because this case "involves direct competitors." *Id.* at 17. But Judge Rawlinson correctly observed that this distinction is illusory, as "the plaintiff in *Zango* asserted similar anticompetition effects." *Id.* at 25; *see also* Reply Br. of Appellant at 10, *Zango*, 568 F.3d 1169 (No. 07-35800) (asserting that the "fundamental deprivation of consumer choice, with resultant harm to Zango, [was] at the heart of [that] suit").

II. THE PANEL'S DECISION UNDERMINES CONGRESSIONAL POLICY IN AN EXCEPTIONALLY IMPORTANT AREA OF LAW.

Even if the majority's focus on policy could be squared with precedent—and it cannot—the majority profoundly misinterpreted how Congress's policy

[4] For example, in an appropriate case, the "good faith" requirement in subparagraph (A) might accomplish this by assuring that a provider reaches its determination in "good faith." Of course, as Malwarebytes has explained, that limitation is unavailable in this case, which involves subparagraph (B) immunity. *Cf. Zango*, 568 F.3d at 1177 (noting that "subparagraph (B) * * * has no good faith language").

considerations apply in this case. Its errors threaten grave consequences for the future of Internet security.

1. The majority believed that its result flowed from the CDA's enumerated policy goals. Seizing especially on one of those goals—preserving "the vibrant and competitive free market" for "Internet * * * services," 47 U.S.C. § 230(b)(2)—the majority expressed concern that providers would rely on "unbridled discretion to block online content" to "drive each other out of business." Add. 17-18. In the majority's view, users would be powerless bystanders with no choice but to "trust that the provider will block material consistent with that user's desires." *Id.* at 18. Judge Fisher, concurring in *Zango*, expressed a similar concern that crafty providers "could employ their software to block content for anticompetitive purposes *without the user's knowledge*." 568 F.3d at 1179.

But, as Malwarebytes has explained, if the majority actually heeded the textual differences between subparagraphs (A) and (B), it would have no need to worry. The kind of immunity that Malwarebytes relies on could not immunize the kind of "covert, anti-competitive blocking" that troubled Judge Fisher, *id.*, and the majority, Add. 18. That immunity applies only to entities that provide "*others* the technical means" to filter content. 47 U.S.C. § 230(c)(2)(B) (emphasis added). If those "others"—in this case, individual users—are unsatisfied with Malwarebytes's filtering technology, they are free to choose a different product.

2. By replacing the scheme that Congress enacted with one of its own devising, the majority has undermined Congress's stated goals. The majority failed to appreciate that many purveyors of unwanted content on the Internet—from deceptive PUPs to viruses to spyware—often *pose* as legitimate security software. *See* Mario Trujillo, *Computer Crimes*, 56 Am. Crim. L. Rev. 615, 622 (2019). Many developers of malicious software subjected to filtering can therefore retaliate by filing lawsuits.

Under the majority's rule, as long a plaintiff can craft allegations that survive relatively minimal pleading standards, the case must proceed at least through discovery to summary judgment.[5] The constant looming threat of costly litigation will chill legitimate security firms from developing technologies capable of filtering the latest threats. As a result, their products will be less competitive and users will have reduced control over the material they receive. *Cf. Zango*, 568 F.3d at 1174 (noting that "more software" for "block[ing] malware" means "more control over the content" for "users"). Thus, the majority's approach actually erects "disincentives for the development * * * of blocking and filtering technologies," thereby reducing "user control" over the flow of information and

[5] The majority exacerbates this problem by setting an extremely low bar for what a putative competitor must allege. It accepts at face value Enigma's claims of "anticompetitive" action without listing any specific facts to support that claim. Add. 20. Any number of future plaintiffs can easily parrot such threadbare allegations.

stifling the "vibrant and competitive free market" for filtration tools. 47 U.S.C. § 230(b)(2)-(4).

The consequences will be widely felt. The "Internet is vital for a wide range of routine activities in today's world[.]" *United States* v. *LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016). Its users need tools to protect themselves from a constantly evolving host of threats. The majority's opinion instead rewards developers who take advantage of users by peddling malware in the guise of security software while hindering legitimate security programs from combating such deceptive actors. That completely inverts the incentives that Congress sought to create—a result that is particularly troubling given this Circuit's status as a hub for technological development.

III. THE PANEL OPINION GIVES POOR GUIDANCE TO DISTRICT COURTS.

Finally, the majority opinion contains language likely to confuse lower courts and spawn even *more* litigation. Although the majority's reasoning focuses chiefly on "anticompetitive" conduct, Add. 20, the opinion also suggests that the statute requires a provider to filter content "based on the characteristics of the online material, *i.e.* its content, and not on the identity of the entity that produced it," *id.* at 10. That sweeping formulation exposes providers to liability for far more than merely anticompetitive conduct. Bad actors are constantly devising new ways to infiltrate computer systems. Read literally, this statement would authorize

litigation if an anti-spyware program blocks new content from a known hacker or if anti-spam filters block mail from a known spammer without assessing each individual email. That cannot be the law. Even if the en banc Court denies review, Malwarebytes urges the panel to grant rehearing to strike this sentence from the opinion.

CONCLUSION

The petition for panel rehearing and rehearing en banc should be granted.

Respectfully submitted,

/s/ Neal Kumar Katyal

TYLER GRIFFIN NEWBY
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Fax: (415) 281-1350
Email: tnewby@fenwick.com

NEAL KUMAR KATYAL
BENJAMIN A. FIELD
REEDY C. SWANSON
HOGAN LOVELLS US LLP
555 Thirteenth Street NW
Washington, DC 20004
Telephone: (202) 637-5600
Fax: (202) 637-5910
Email: neal.katyal@hoganlovells.com

Attorneys for Defendant-Appellee Malwarebytes, Inc.

Dated: October 28, 2019

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 11. Certificate of Compliance for Petitions for Rehearing or Answers

Instructions for this form: http://www.ca9.uscourts.gov/forms/form11instructions.pdf

9th Cir. Case Number(s) 17-17351

I am the attorney or self-represented party.

I certify that pursuant to Circuit Rule 35-4 or 40-1, the attached petition for panel rehearing/petition for rehearing en banc/answer to petition is (*select one*):

◉ Prepared in a format, typeface, and type style that complies with Fed. R. App. P. 32(a)(4)-(6) and **contains the following number of words**: 4,193.

(Petitions and answers must not exceed 4,200 words)

OR

○ In compliance with Fed. R. App. P. 32(a)(4)-(6) and does not exceed 15 pages.

Signature /s/ Neal Kumar Katyal **Date** Oct 28, 2019

*(use "*s/[typed name]*" to sign electronically-filed documents)*

ADDENDUM

TABLE OF CONTENTS

Page

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ENIGMA SOFTWARE GROUP USA, LLC, *Plaintiff-Appellant*, v. MALWAREBYTES, INC., *Defendant-Appellee.*	No. 17-17351 D.C. No. 5:17-cv-02915-EJD OPINION

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.

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 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 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

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

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, 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).[1]

[1] 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).

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 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 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.

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.

SUPERIOR COURT, STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

Department 1, Honorable Brian C. Walsh Presiding

JeeJee Vizconde, Courtroom Clerk
191 North First Street, San Jose, CA 95113
Telephone: 408.882.2150

To contest the ruling, call (408) 808-6856 before 4:00 P.M.
Please state your case name, case number, the name of the attorney and contact number. It would also be helpful if you could identify the specific portion or portions of the tentative ruling that will be contested. Thank you.

Court Reporters are not provided. Please consult our Court's website, www.scscourt.org, for the rules, policies and required forms for the court's appointment by stipulation of privately-retained court reporters.

LAW AND MOTION TENTATIVE RULINGS
DATE: OCTOBER 25, 2019 TIME: 9 A.M.
PREVAILING PARTY SHALL PREPARE THE ORDER
(SEE RULE OF COURT 3.1312)

LINE #	CASE #	CASE TITLE	RULING
LINE 1	19CV340667	Prager University vs. Google LLC, et al	CLICK on LINE 1 for Ruling.
LINE 2	19CV341522	In Re Alphabet, Inc. Shareholder Derivative Litigation [LEAD CASE; Consolidated with Case Nos. 19CV343670, 19CV343672, 19CV344792, 19CV346737]	CLICK on LINE 2 for Ruling.
LINE 3	17CV315727	Hancock vs. Magnolia HI-Fi LLC, et al	CLICK on LINE 3 for Ruling.
LINE 4	19CV348674	In Re Cloudera, Inc. Securities Litigation (formerly Lazard vs. Cloudera Inc., et al) LEAD CASE / Consolidated Action	CLICK on LINE 4 for Ruling.
LINE 5	19CV347622	InESS Solutions, Inc. vs. Cisco Systems Inc.	OFF CALENDAR
LINE 6			
LINE 7			
LINE 8			
LINE 9			
LINE 10			
LINE 11			
LINE 12			

SUPERIOR COURT, STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

Department 1, Honorable Brian C. Walsh Presiding

JeeJee Vizconde, Courtroom Clerk
191 North First Street, San Jose, CA 95113
Telephone: 408.882.2150

To contest the ruling, call (408) 808-6856 before 4:00 P.M.
Please state your case name, case number, the name of the attorney and contact number. It would also be helpful if you could identify the specific portion or portions of the tentative ruling that will be contested. Thank you.

Court Reporters are not provided. Please consult our Court's website, www.scscourt.org, for the rules, policies and required forms for the court's appointment by stipulation of privately-retained court reporters.

LAW AND MOTION TENTATIVE RULINGS

LINE 13			

Calendar Line 1

Case Name: *Prager University v. Google LLC, et al.*
Case No.: 19-CV-340667

This action arises from Prager University's allegations that YouTube, LLC and its parent company Google LLC have unlawfully restricted content created by Prager on YouTube, defendants' social media and video sharing platform. Before the Court are defendants' demurrer to the operative First Amended Complaint ("FAC") and Prager's motion for a preliminary injunction. Both motions are opposed.

I. Factual and Procedural Background

As alleged in the FAC, Prager is a non-profit, 501(c)(3) tax exempt, educational organization that promotes discussion on historical, religious, and current events by disseminating educational videos intended for younger, student-based audiences between the ages of 13 and 35. (FAC, ¶ 10.) The videos depict scholars, sources, and other prominent speakers who often espouse viewpoints in the mainstream of conservative thought. (*Ibid.*)

Defendants operate YouTube as the largest and most profitable mechanism for monetizing free speech and freedom of expression in the history of the world, generating $10 to 15 billion in annual revenue by monetizing the content of users like Prager who are invited to post videos to YouTube. (FAC, ¶ 11.) Since its inception, Prager has posted more than 250 of its videos to YouTube. (*Id.* at ¶ 39.)

A. The Alleged Content Restriction Scheme

To induce users like Prager to upload video content, defendants represent that YouTube is a public place for free speech defined by "four essential freedoms" that govern the public's use of the platform:

1. **Freedom of Expression:** We believe people should be able to speak freely, share opinions, foster open dialogue, and that creative freedom leads to new voices, formats and possibilities.

2. **Freedom of Information:** We believe everyone should have easy, open access to information and that video is a powerful force for education, building understanding, and documenting world events, big and small.

3. **Freedom of Opportunity:** We believe everyone should have a chance to be discovered, build a business and succeed on their own terms, and that people—not gatekeepers—decide what's popular.

4. **Freedom to Belong:** We believe everyone should be able to find communities of support, break down barriers, transcend borders and come together around shared interests and passions.

(FAC, ¶ 12.) Defendants further promise that YouTube is governed by content-based rules and filtering which "apply equally to all," regardless of the viewpoint, identity, or source of the speaker. (*Id.* at ¶ 13.)

However, contrary to these representations, defendants censor, restrict, and restrain video content based on animus, discrimination, profit, and/or for any other reason "or no reason." (FAC, ¶ 14.) According to Prager, an internal memo and presentation entitled "The Good Censor" shows that defendants have secretly decided to " 'migrate' away from [serving as] a hosting platform …where the public is invited to engage in freedom of expression" to become a media company that profits "by promoting Defendants' own, or their preferred content through the exercise of unfettered discretion to censor and curate otherwise public content." (*Id.* at ¶¶ 56-65.) To effectuate their discriminatory practices, defendants use clandestine filtering tools, including algorithms and other machine-based and manual review tools, that are embedded with discriminatory and anti-competitive animus-based code, including code that is used to identify and restrict content based on the identity, viewpoint, or topic of the speaker. (*Id.*, ¶ 19.) They also "ensure that the YouTube employees charged with administering the content filtering and regulation scheme … operate in a dysfunctional and politically partisan workplace environment." (*Id.* at ¶ 20.)

Against this background, Prager's rights under California law have been violated by two unlawful content-based restrictions: (i) "Restricted Mode," a filtering protocol that defendants use to block what they deem, in their sole, unfettered discretion, to be "inappropriate" for "sensitive" audiences and (ii) "Advertising Restrictions," a content-based video advertising restriction policy that prohibits potential advertisers from accessing videos that defendants deem "inappropriate" for advertising. (FAC, ¶ 17.) Defendants use these mechanisms as a pretext to restrict and censor Prager's videos, even though the content of its videos complies with YouTube's Terms of Service, Community Guidelines, and criteria for "sensitive audiences" and advertisers, while they fail to restrict the content of other preferred users, content partners, and content produced by defendants themselves that is not compliant. (*Id.* at ¶¶ 18, 23.) Defendants have provided no rational basis for restricting Prager's content while allowing similar or noncompliant content to go unrestricted. (*Id.* at ¶ 25.)

B. Restricted Mode

According to defendants, Restricted Mode is intended "to help institutions like schools as well as people who wanted to better control the content they see on YouTube with an option to choose an intentionally limited YouTube experience." (FAC, ¶ 68.) Viewers can choose to turn Restricted Mode on from their personal accounts, but it may also be turned on by system administrators for libraries, schools, and other institutions or workplaces. (*Ibid.*) Defendants estimate that about 1.5 percent of YouTube's daily views (or approximately 75 million views per day) come from individuals using Restricted Mode. (*Id.* at ¶ 69.) When Restricted Mode is activated, a video's name, creator or subject, and content, along with any other information related to the video, are blocked, as if the video did not exist on the YouTube platform. (*Id.* at ¶ 68.)

Defendants claim to restrict content in Restricted Mode based upon their "Restricted Mode Guidelines," which identify five criteria for determining whether content warrants restriction:

1. Talking about drug use or abuse, or drinking alcohol in videos;
2. Overly detailed conversations about or depictions of sex or sexual activity;
3. Graphic descriptions of violence, violent acts, natural disasters and tragedies, or even violence in the news;
4. Videos that cover specific details about events related to terrorism, war, crime, and political conflicts that resulted in death or serious injury, even if no graphic imagery is shown;
5. Inappropriate language, including profanity; and
6. Video content that is gratuitously incendiary, inflammatory, or demeaning towards an individual or group.

(FAC, ¶ 70.) Videos are initially restricted through an automated filtering algorithm that examines certain "signals" like the video's metadata, title, and language, or following manual review if a video is "flagged" as inappropriate by public viewers. (*Id.*, ¶ 71.)

YouTube also publishes "Community Guidelines" and "Age Based Restriction" guidelines similar to its "Restricted Mode Guidelines"; however, content that complies with these guidelines may nevertheless be subject to Restricted Mode. (FAC, ¶¶ 72-73.) Prager's videos have never been age restricted or found to violate YouTube's Community Guidelines. (*Id.* at ¶ 75.)

Defendants have admitted that they make "mistakes in understanding context and nuances when [assessing] which videos to make available in Restricted Mode." (FAC, ¶ 91.) For example, on March 19, 2017, they publicly admitted that they improperly restricted videos posted or produced by members of the LGBTQ community and changed their policy, filtering algorithm, and manual review policies in response to complaints from this community. (*Id.* at ¶¶ 94-96.) However, Prager alleges that defendants have continued to improperly restrict videos by LGBTQ users, which is evidence of viewpoint animus. (*Id.* at ¶¶ 97-98.)

C. Advertising Restrictions

Defendants also restrict users like Prager "from monetizing or boosting the reach or viewer distribution of [their] videos." (FAC, ¶ 78.) Prager alleges that these restrictions are ostensibly governed by the "AdSense program policies," which it suggests are "similar[ly] vague, ambiguous, and arbitrary" to the Restricted Mode Guidelines. (*Id.* at ¶¶ 78, 80.) Prager claims that, similar to their "mistakes" in applying "Restricted Mode," defendants once "denied a reach boost or ad product" on the ground of "shocking content" based on a user's sexual or gender orientation and viewpoint. (*Id.* at ¶ 81.) It alleges that the application of such an "inappropriate" or "shocking content" designation falsely and unfairly stigmatizes Prager as well. (*Id.* at ¶ 82.) (However, while Prager alleges that certain of its videos have been demonetized, it does not allege whether defendants gave specific reasons for these actions or what those reasons were.) (See *id.* at ¶ 84.)

D. The Parties' Dispute

In July of 2016, Prager discovered that defendants were restricting user access to its videos through Restricted Mode. (FAC, ¶ 101.) It raised the issue with defendants, but they have failed to offer any reasonable or consistent explanation for why Prager's videos are being restricted. (*Id.* at ¶¶ 101-117.) In 2016, at least 16 Prager videos were restricted; by 2017, a

total of 21 were. (*Ibid.*) By the time the FAC was filed in May of 2019, the total had risen to 80. (*Id.* at ¶ 127.) Prager's videos were either "restricted as to content, demonetized, or both." (*Id.* at ¶ 116.) Defendants also discontinued Prager's "ad grants" account for more than six days in October of 2017. (*Id.* at ¶ 118.) On pages 9-17 of the FAC, Prager provides a chart listing its restricted videos by title, along with videos from defendants' "preferred content providers" with similar titles that are unrestricted. (*Id.* at ¶ 23.)

On October 23, 2017, Prager sued defendants in federal court, asserting claims for (1) violation of Article I, section 2 of the California Constitution; (2) violation of the First Amendment of the United States Constitution; (3) violation of the California Unruh Civil Rights Act ("Unruh Act"), Cal. Civ. Code. § 51 *et seq.*; (4) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200 *et seq.*; (5) breach of the implied covenant of good faith and fair dealing; (6) violation of the Lanham Act, 15 U.S.C. § 1125 *et seq.*; and (7) declaratory relief. (*Prager University v. Google LLC* (N.D. Cal., Mar. 26, 2018, No. 17-CV-06064-LHK) 2018 WL 1471939, at *2.) It filed a motion for a preliminary injunction in the federal action on December 29, 2017. (*Id.* at *3.) On March 26, 2018, the federal court granted defendants' motion to dismiss Prager's federal claims and denied Prager's motion for a preliminary injunction, finding that Prager had failed to state a claim for violation of the First Amendment because it did not allege state action, and had also failed to state a claim under the Lanham Act. (*Id.* at *5-13.) Having dismissed all of Prager's federal claims, the court declined to exercise supplemental jurisdiction over its state law claims, explaining:

> Here, the factors of economy, convenience, fairness, and comity support dismissal of Plaintiff's remaining state law claims. This case is still at the pleading stage, and no discovery has taken place. Federal judicial resources are conserved by dismissing the state law theories of relief at this stage. Further, the Court finds that dismissal promotes comity as it enables California courts to interpret questions of state law. This is an especially important consideration in the instant case because Plaintiff asserts a claim that demands an analysis of the reach of Article I, section 2 of the California Constitution in the age of social media and the Internet.

(*Prager University v. Google LLC*, *supra,* 2018 WL 1471939, at *13.) Prager has appealed the federal court's ruling to the Court of Appeal for the Ninth Circuit, which heard argument in the matter on August 27, 2019.

Prager filed this action on January 8, 2019, reasserting its state law claims for (1) violation of Article I, section 2 of the California Constitution; (2) violation of the Unruh Act; (3) violation of the UCL; and (4) breach of the implied covenant of good faith and fair dealing. On May 13, the Court entered a stipulated order establishing a briefing schedule for Prager's anticipated motion for a preliminary injunction and defendants' anticipated demurrer and/or special motion to strike. On May 20, pursuant to that order, Prager moved for a preliminary injunction and filed the FAC, which asserts the same four causes of action as its original complaint. Defendants filed their demurrer on June 28. Both matters are now fully briefed and have come on for hearing by the Court.

II. Demurrer to the FAC

Defendants demur to each cause of action in the FAC for failure to state a claim. (Code Civ. Proc., § 430.10, subd. (e).) They contend that Prager's claims are barred by two provisions of section 230 of the Communications Decency Act (the "CDA") and by the First Amendment, and otherwise fail to state a cause of action.

Defendants' request for judicial notice, which is unopposed, is GRANTED as to public web pages displaying the terms of the various YouTube policies at issue in this action (Exhibits 1-9). (Evid. Code § 452, subd. (h); see *Pacific Employers Ins. Co. v. State of Cal.* (1970) 3 Cal.3d 573, 575, fn.1 [where portions of agreement were attached to plaintiff's complaint, the balance of that agreement was properly a subject of judicial notice]; *Ingram v. Flippo* (1999) 74 Cal.App.4th 1280, 1285 [judicial notice of letter and media release was proper where, although they were not attached to the complaint, they formed a basis for the claims, and the complaint excerpted quotes and summarized parts in detail, thus "it is essential that we evaluate the complaint by reference to these documents"].) Defendants' request is also GRANTED as to a transcript of a case management conference held in the federal action, although the Court is not bound by the court's comments or rulings in that case. (Evid. Code § 452, subd. (d).)

A. Legal Standard

The function of a demurrer is to test the legal sufficiency of a pleading. (*Trs. Of Capital Wholesale Elec. Etc. Fund v. Shearson Lehman Bros.* (1990) 221 Cal.App.3d 617, 621.) Consequently, "[a] demurrer reaches only to the contents of the pleading and such matters as may be considered under the doctrine of judicial notice." (*South Shore Land Co. v. Petersen* (1964) 226 Cal.App.2d 725, 732, internal citations and quotations omitted; see also Code Civ. Proc., § 430.30, subd. (a).) "It is not the ordinary function of a demurrer to test the truth of the plaintiff's allegations or the accuracy with which he describes the defendant's conduct. … Thus, … the facts alleged in the pleading are deemed to be true, however improbable they may be." (*Align Technology, Inc. v. Tran* (2009) 179 Cal.App.4th 949, 958, internal citations and quotations omitted.)

In ruling on a demurrer, the allegations of the complaint must be liberally construed, with a view to substantial justice between the parties. (*Glennen v. Allergan, Inc.* (2016) 247 Cal.App.4th 1, 6.) Nevertheless, while "[a] demurrer admits all facts properly pleaded, [it does] not [admit] contentions, deductions or conclusions of law or fact." (*George v. Automobile Club of Southern California* (2011) 201 Cal.App.4th 1112, 1120.) A demurrer will lie where the allegations and matters subject to judicial notice clearly disclose some defense or bar to recovery, including a statutory immunity. (*Casterson v. Superior Court (Cardoso)* (2002) 101 Cal.App.4th 177, 183.)

B. Violation of the California Constitution

Because concepts related to the parties' speech rights under the First Amendment and California Constitution are important to other aspects of its analysis, the Court will first examine whether Prager states a claim for violation of Article I, section 2 of the California Constitution.

As urged by defendants, "California's free speech clause"—like the First Amendment—"contains a state action limitation." (*Golden Gateway Center v. Golden Gateway Tenants Assn.* (2001) 26 Cal.4th 1013, 1023.) However, the California Constitution's protection of speech has been interpreted more broadly in this regard. (See *Fashion Valley Mall, LLC v. National Labor Relations Bd.* (2007) 42 Cal.4th 850, 862-863.) Most notably, in the "groundbreaking" decision of *Robins v. Pruneyard Shopping Center* (1979) 23 Cal.3d 899, the Supreme Court of California "departed from the First Amendment jurisprudence of the United States Supreme Court and extended the reach of the free speech clause of the California Constitution to privately owned shopping centers." (*Golden Gateway Center v. Golden Gateway Tenants Assn.*, *supra,* 26 Cal.4th at p. 1016.)

More than 20 years after *Robins v. Pruneyard*, *Golden Gateway Center* confirmed and began to define the scope of the state action limitation under the California Constitution, finding the requirement was not satisfied where a tenants' association sought to distribute leaflets in a private apartment complex that was "not freely open to the public." (*Golden Gateway Center v. Golden Gateway Tenants Assn.*, *supra,* 26 Cal.4th at p. 1031.) *Golden Gateway Center* looked to the reasoning of *Robins* for guidance, noting that "*Robins* relied heavily on the functional equivalence of the shopping center to a traditional public forum-the downtown or central business district," and relied on "the public character of the property," emphasizing "the public's unrestricted access." (*Id.* at pp. 1032-1033, internal citations and quotations omitted.) *Golden Gateway Center* held that this unrestricted access is a "threshold requirement for establishing state action": without it, private property "is not the functional equivalent of a traditional public forum." (*Id.* at p. 1033.) In announcing this requirement, the opinion confirmed that it "largely follow[ed] the Court of Appeal decisions construing *Robins*," including *Planned Parenthood v. Wilson* (1991) 234 Cal.App.3d 1662. (*Id.* at p. 1033.) Those decisions also emphasized *Robins*'s focus on "the unique character of the modern shopping center and … the public role such centers have assumed in contemporary society" by effectively replacing "the traditional town center business block, where historically the public's First Amendment activity was exercised and its right to do so scrupulously guarded." (*Planned Parenthood v. Wilson*, *supra,* 234 Cal.App.3d at pp. 1669-1670.) This concept was again emphasized by the California Supreme Court in *Fashion Valley*, which repeatedly referenced "[t]he idea that private property can constitute a public forum for free speech if it is open to the public in a manner similar to that of public streets and sidewalks …." (*Fashion Valley Mall, LLC v. National Labor Relations Bd.*, *supra,* 42 Cal.4th at p. 858; see also *id.* at p. 859.)

With this fundamental principle in mind, it is apparent that Prager does not state a claim under the California Constitution. Prager contends that "YouTube is the cyber equivalent of a town square where citizens exchange ideas on matters of public interest" and that defendants have opened their platform to the public by advertising its use for this purpose. However, Prager does not allege that it has been denied access to the core YouTube service. Rather, it urges that its access to "Restricted Mode" and YouTube's advertising service has been restricted. Prager does not persuade the Court that these services are freely open to the public or are the functional equivalent of a traditional public forum like a town square or a central business district.[1] Considering "the nature, purpose, and primary use of the property; the

[1] Prager cites no authority that supports its position that a court can never determine the applicability of *Robins* on demurrer, and this position is incorrect. (See *Savage v. Trammell Crow Co.* (1990) 223 Cal.App.3d 1562, 1577,

extent and nature of the public invitation to use the property; and the relationship between the ideas sought to be presented and the purpose of the property's occupants" (*Albertson's, Inc. v. Young* (2003) 107 Cal.App.4th at p. 119), it is clear that these services are nothing like a traditional public forum. "Restricted Mode" is an optional service that enables users to limit the content that they (or their children, patrons, or employees) view in order to avoid mature content. Limiting content is the very purpose of this service, and defendants do not give content creators unrestricted access to it or suggest that they will do so. The service exists to permit users to avoid the more open experience of the core YouTube service. Similarly, the use of YouTube's advertising service is restricted to meet the preferences of advertisers. (See FAC, ¶ 80 [stated purpose of advertising restrictions "is to keep Google's content and search networks safe and clean for our advertisers …"]; Declaration of Brian M. Willen, Exs. 7-9.)

Defendants correctly urge that even to recognize the core YouTube platform as a public forum would be a dramatic expansion of *Robins*. As one federal court observed, "[t]he analogy between a shopping mall and the Internet is imperfect, and there are a host of potential 'slippery slope' problems that are likely to surface were [*Robins*] to apply to the Internet." (*hiQ Labs, Inc. v. LinkedIn Corporation* (N.D. Cal. 2017) 273 F.Supp.3d 1099, 1116 [observing that "[n]o court has expressly extended [*Robins*] to the Internet generally"], *aff'd and remanded* (9th Cir. 2019) 938 F.3d 985.) However the courts of this state ultimately view that analogy with regard to a dominant, widely-used site like the core YouTube service, the analogy falls apart completely on the facts alleged here. "Restricted Mode" and YouTube's advertising service are new, inherently selective platforms that do not resemble a traditional public forum. As discussed below, even more than the core YouTube service, these platforms necessarily reflect the exercise of editorial discretion rather than serving as an open "town square."

Finally, Prager contends that cases that have deemed web sites to be "public forums" for purposes of California's "anti-SLAPP" statute require this Court to extend *Robins* to its claim. However, the anti-SLAPP statute encompasses speech "***in a place open to the public or*** a public forum in connection with an issue of public interest" (Code Civ. Proc., § 425.16, subd. (e)(3), emphasis added), and has been applied to locations that clearly do not meet the standard described in *Golden Gateway Center*. (See, e.g., *Seelig v. Infinity Broadcasting Corp.* (2002) 97 Cal.App.4th 798, 807 [anti-SLAPP statute applied to comments made during on-air discussion on talk radio].) "[T]he protections afforded by the anti-SLAPP statute are not coextensive with the categories of conduct or speech protected by the First Amendment or its California counterparts (Cal. Const., art. I, §§ 2–4)." (*Industrial Waste & Debris Box Service, Inc. v. Murphy* (2016) 4 Cal.App.5th 1135, 1152.) "As our high court recently reaffirmed, 'courts determining whether conduct is protected under the anti-SLAPP statute look not to First Amendment law, but to the statutory definitions in section 425.16, subdivision (e).' " (*Ibid.*, quoting *City of Montebello v. Vasquez* (2016) 1 Cal.5th 409, 422.)

Defendants' demurrer to the first cause of action will accordingly be sustained without leave to amend. In addition to failing to state a claim under *Robins v. Pruneyard*, this cause of action is barred by section 230 of the CDA for the reasons discussed below. (See *In re Garcia* (2014) 58 Cal.4th 440, 452 [supremacy clause of the federal Constitution requires that any conflicting state law give way to federal statute], citing U.S. Const., art. VI, cl. 2 ["This

---

fn. 4 [stating that scope of *Robins* can be addressed on demurrer in appropriate circumstances].) Here, the necessary facts are alleged in the FAC and/or subject to judicial notice.

Constitution, and the laws of the United States which shall be made in pursuance thereof ... shall be the supreme law of the land; and the judges in every state shall be bound thereby, any thing in the Constitution or laws of any state to the contrary notwithstanding"].)

B. CDA Immunity

Section 230(c)(1) of the CDA provides 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." "§ 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred." (*Hassell v. Bird* (2018) 5 Cal.5th 522, 536, quoting *Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327, 330.)

"The CDA—of which section 230 is a part—was enacted in 1996." (*Delfino v. Agilent Technologies, Inc.* (2006) 145 Cal.App.4th 790, 802.) "Its 'primary goal ... was to control the exposure of minors to indecent material' over the Internet." (*Ibid.*, quoting *Batzel v. Smith* (9th Cir. 2003) 333 F.3d 1018, 1026, superseded by statute on another point as stated in *Breazeale v. Victim Services, Inc.* (9th Cir. 2017) 878 F.3d 759, 766.) "Thus, an 'important purpose of [the CDA] was to encourage [Internet] service providers to self-regulate the dissemination of offensive materials over their services.' " (*Ibid.*, quoting *Zeran v. America Online, Inc., supra,* 129 F.3d at p. 331.) Section 230(c)(2) consequently immunizes service providers[2] who endeavor to restrict access to material deemed objectionable, providing that

> [n]o 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).[3]

(47 U.S.C. § 230(c)(2).)

A second, but related, objective of the CDA "was to avoid the chilling effect upon Internet free speech that would be occasioned by the imposition of tort liability upon companies that do not create potentially harmful messages but are simply intermediaries for their delivery." (*Delfino v. Agilent Technologies, Inc.*, *supra,* 145 Cal.App.4th at pp. 802-803.)

---

[2] There is no dispute that defendants are providers of "an interactive computer service" under section 230.

[3] It is widely agreed that section 230(c)(2)(B)'s reference to "paragraph (1)" is an error, and the provision should be interpreted to refer to section 230(c)(2)(A) or "paragraph (A)." (See, e.g., *Enigma Software Group USA, LLC v. Malwarebytes, Inc.* (9th Cir. 2019) 938 F.3d 1026, 1031, fn. 1.)

The legislative history reflects that Congress was responding to a New York trial court case where "a service provider was held liable for defamatory comments posted on one of its bulletin boards, based on a finding that the provider had adopted the role of 'publisher' by actively screening and editing postings." (*Barrett v. Rosenthal* (2006) 40 Cal.4th 33, 44.) " 'Fearing that the specter of liability would ... deter service providers from blocking and screening offensive material,' " Congress forbid " 'the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.' " (*Id.*, quoting *Zeran v. America Online, Inc., supra,* 129 F.3d at p. 331.) Thus, section 230(c)(1) " 'confer[s] broad immunity on Internet intermediaries' " in " 'a strong demonstration of legislative commitment to the value of maintaining a free market for online expression.' " (*Hassell v. Bird*, *supra,* 5 Cal.5th at p. 539, quoting *Barrett v. Rosenthal*, *supra,* 40 Cal.4th at p. 56.)

Of the two provisions, section 230(c)(1) has been applied more frequently and broadly, including by courts in the Northern District of California to conduct indistinguishable from that alleged in this action. Notably, in *Sikhs for Justice "SFJ", Inc. v. Facebook, Inc.* (N.D. Cal. 2015) 144 F.Supp.3d 1088, 1090, *aff'd sub nom. Sikhs for Justice, Inc. v. Facebook, Inc.* (9th Cir. 2017) 697 Fed.App'x. 526, a human rights organization alleged that Facebook blocked access to its page in India "on its own or on the behest of the Government of India," because of discrimination on the grounds of race, religion, ancestry, and national origin. Quoting *Barnes v. Yahoo!, Inc.* (9th Cir. 2009) 570 F.3d 1096 and *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC* (9th Cir. 2008) 521 F.3d 1157, the court reasoned that

> [p]ublication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content. Thus, a publisher decides whether to publish material submitted for publication. It is immaterial whether this decision comes in the form of deciding what to publish in the first place or what to remove among the published material. ***In other words, any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230.***

(*Sikhs for Justice "SFJ", Inc. v. Facebook, Inc.*, *supra,* 144 F.Supp.3d at p. 1094, emphasis added, internal citations and quotations omitted.) This approach has been endorsed by the Ninth Circuit. (See *Riggs v. MySpace, Inc.* (9th Cir. 2011) 444 Fed.App'x. 986, 987 [district court properly dismissed claims "arising from MySpace's decisions to delete Riggs's user profiles on its social networking website yet not delete other profiles Riggs alleged were created by celebrity imposters," citing *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, *supra,* 521 F.3d at pp. 1170-1171 for the proposition that "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230"].) California opinions have similarly reasoned that the "type of activity" at issue here—"to restrict or make available certain material"—"is expressly covered by section 230." (*Doe II v. MySpace Inc.* (2009) 175 Cal.App.4th 561, 572-573 [describing "the general consensus to interpret section 230 immunity broadly, extending from *Zeran* …"]; see also *Hassell v. Bird, supra,* 5 Cal.5th at p. 537 [California "courts have followed *Zeran* in adopting a broad view of section 230's immunity provisions"].) This interpretation was recently applied again by the Northern District in *Federal Agency of News LLC v. Facebook, Inc.* (N.D. Cal., July 20, 2019, No. 18-CV-07041-LHK) --- F.Sup.3d ---, 2019 WL 3254208, where it was held that section 230(c)(1) immunized Facebook from claims

arising from its removal of a Russian company's account and page due to its alleged control by an entity found to have interfered in the 2016 United States presidential election.[4]

Consistent with the language of section 230(c)(1), these cases do not question the service provider's motive in deciding to remove content from its service. While Prager contends that section 230(c)(1) immunity should not be applied where a plaintiff alleges a service provider acted in bad faith or to stifle competition, it cites no persuasive authority adopting this interpretation.[5]

Courts have expressed greater concern with the issue of motive when interpreting section 230(c)(2), perhaps because paragraph (A) of that provision expressly includes a "good faith" requirement. Here, defendants rely on paragraph (B) of that provision, which they urge—like section 230(c)(1)—does not require good faith. In *Zango, Inc. v. Kaspersky Lab, Inc.* (9th Cir. 2009) 568 F.3d 1169, 1176-1177, the Ninth Circuit applied section 230(c)(2)(B) to a provider of Internet security software that deemed the plaintiff's software to be "malware," noting that the plaintiff had waived the issue of "whether subparagraph (B), which has no good faith language, should be construed implicitly to have a good faith component like

---

[4] See also *Langdon v. Google, Inc.* (D. Del. 2007) 474 F.Supp.2d 622, 630-631 (applying immunity under section 230(c)(1) and/or (2) where plaintiff alleged defendants refused to display ads on his web pages criticizing the North Carolina and Chinese governments based on political viewpoint discrimination); *Levitt v. Yelp! Inc.* (N.D. Cal., Oct. 26, 2011, No. C-10-1321 EMC) 2011 WL 5079526, at *7-9, *aff'd* (9th Cir. 2014) 765 F.3d 1123 (section 230(c)(1) immunity applied to allegations that Yelp manipulated plaintiffs' user reviews in order to induce them to pay for advertising); *Lancaster v. Alphabet Inc.* (N.D. Cal., July 8, 2016, No. 15-CV-05299-HSG) 2016 WL 3648608, at *2-3 ("§ 230[(c)(1) of the CDA prohibits any claim arising from Defendants' removal of Plaintiffs' videos"); *Green v. YouTube, LLC* (D.N.H., Mar. 13, 2019, No. 18-CV-203-PB) 2019 WL 1428890, at *6, *report and recommendation adopted sub nom. Green v. YouTube, Inc.* (D.N.H., Mar. 29, 2019, No. 18-CV-203-PB) 2019 WL 1428311 (applying immunity under section 230(c)(1) where plaintiff alleged his accounts were improperly shut down); *Brittain v. Twitter, Inc.* (N.D. Cal., June 10, 2019, No. 19-CV-00114-YGR) 2019 WL 2423375, at *3 (section 230(c)(1) immunity applied where plaintiff alleged improper suspension of his Twitter accounts and that Twitter "limit[ed] users who reference new/competing networks and/or utilize Third Party API services"); *King v. Facebook, Inc.* (N.D. Cal., Sept. 5, 2019, No. 19-CV-01987-WHO) 2019 WL 4221768 (section 230(c)(1) immunity applied to theory that "Facebook has violated its (Terms of Service] in removing [plaintiff's] posts and suspending his account, and that Facebook treats black activists and their posts differently than it does other groups, particularly white supremacists and certain 'hate groups' ").

[5] To the extent *e-ventures Worldwide, LLC v. Google, Inc.* (M.D. Fla. 2016) 188 F.Supp.3d 1265 adopts Prager's view, it does so by conflating section 230(c)(1) and section 230(c)(2) with no analysis. The Court does not find this persuasive. While a subsequent, unpublished opinion in that action, *e-ventures Worldwide, LLC v. Google, Inc.* (M.D. Fla., Feb. 8, 2017, No. 214CV646FTMPAMCM) 2017 WL 2210029, *3-4 reasoned that applying section 230(c)(1) to service providers' editorial decisions regarding a plaintiff's own content would swallow "the more specific immunity in (c)(2)" with its good faith requirement, the opinion went on to grant summary judgment based on the First Amendment's protection of editorial judgments, "no matter the motive." This case does not persuade the Court to part ways with the courts that apply section 230(c)(1) to the same end based on the same reasoning.

Similarly, *Levitt v. Yelp! Inc.* (N.D. Cal., Mar. 22, 2011, No. C 10-1321 MHP) 2011 WL 13153230, at *9 deemed it "a[] close[] question … whether Yelp may be held liable for its removal of positive reviews for the alleged purpose of coercing businesses to purchase advertising," considering that this theory implicated bad faith. The court ultimately did not resolve the issue as it found the complaint otherwise failed to state a cause of action. A subsequent opinion in that case, *Levitt v. Yelp! Inc.* (N.D. Cal., Oct. 26, 2011, No. C-10-1321 EMC) 2011 WL 5079526, *9 held that section 230(c)(1) does not include a good faith requirement, and applied "even assuming Plaintiffs have adequately pled allegations stating a claim of an extortionate threat with respect to Yelp's alleged manipulation of user reviews." The Court finds the reasoning of the subsequent opinion more persuasive.

subparagraph (A)." The concurring opinion expressed concern with extending immunity beyond the facts present in that case:

> Congress plainly intended to give computer users the tools to filter the Internet's deluge of material *users* would find objectionable, in part by immunizing the providers of blocking software from liability. *See* § 230(b)(3). But under the generous coverage of § 230(c)(2)(B)'s immunity language, a blocking software provider might abuse that immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material "otherwise objectionable."

(*Zango, Inc. v. Kaspersky Lab, Inc.*, *supra,* 568 F.3d at p. 1178 (conc. opn. of Fisher, J.).) Noting that "[d]istrict courts nationwide have grappled with the issues discussed in *Zango*'s majority and concurring opinions, and have reached differing results," the Ninth Circuit recently held that a service provider's intent may be relevant under section 230(c)(2)(B): specifically, where a plaintiff alleges blocking by a direct competitor for anticompetitive purposes, its claims survive dismissal. (*Enigma Software Group USA, LLC v. Malwarebytes, Inc.* (9th Cir. 2019) 938 F.3d 1026.)

Here, defendants' creation of a "Restricted Mode" to allow sensitive users to voluntarily choose a more limited experience of the YouTube service is exactly the type of self-regulation that Congress sought to encourage in enacting section 230, and fits within section 230(c)(2)(B)'s immunity for "any action taken to enable or make available to … others," namely, YouTube users, "the technical means to restrict access to" material "that the provider or user considers to be obscene, … excessively violent, … or otherwise objectionable." Rather than unilaterally restricting access to material on its core platform as contemplated by section 230(c)(2)(A)—which contains a "good faith" requirement—defendants allow users to voluntarily restrict access to material that defendants deem objectionable for the stated reason that, like the categories of material enumerated by the statute, it may be inappropriate for young or sensitive viewers.[6] The Court views this as a critical difference between the two provisions and disagrees with the majority in *Enigma*,[7] who ignore the plain language of the statute by reading a good faith limitation into section 230(c)(2)(B). (See *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, *supra,* 938 F.3d at p. 1040 (dis. opn. of Rawlinson, J.) ["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. [Citation.] 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.' "].)

---

[6] Consistent with these circumstances, a page discussing options for administrators employing "Restricted Mode," which was submitted by Prager in connection with its motion for preliminary injunction, indicates that "[a]dministrators and designated approvers can now whitelist entire channels," in addition to individual videos, to ensure a channel is "watchable by your users." (Declaration of Peter Obstler, Ex. L.) Thus, it appears that users can specifically override defendants' decisions to disable certain videos or channels in "Restricted Mode," confirming that "Restricted Mode" is a tool made available to users rather than a unilateral ban.

[7] See *People v. Williams* (1997) 16 Cal.4th 153, 190 ("Decisions of lower federal courts interpreting federal law are not binding on state courts."); *Elliott v. Albright* (1989) 209 Cal.App.3d 1028, 1034 (although at times entitled to great weight, the decisions of the lower federal courts on federal questions are merely persuasive).

Finding CDA immunity here is also consistent with cases that apply it in indistinguishable circumstances based on section 230(c)(1), and with their reasoning, which recognizes that challenges to a service provider's editorial discretion "treat[]" the provider "as a publisher." (See *Sikhs for Justice "SFJ", Inc. v. Facebook, Inc.*, *supra,* 144 F.Supp.3d 1088 [applying section 230(c)(1) to claim under Title II of the Civil Rights Act of 1964]; *Federal Agency of News LLC v. Facebook, Inc.*, *supra,* 2019 WL 3254208 [applying section 230(c)(1) to claims under Title II of the Civil Rights Act of 1964, the Unruh Act, and for breach of the implied covenant of good faith and fair dealing].) The Court finds that immunity under section 230(c)(1) also applies here, to the allegations involving both "Restricted Mode" and defendants' advertising service.

While the Court understands Prager's argument that all three provisions of section 230 should have a good faith requirement, this argument is contrary to the plain language of the statute. (See *Hassell v. Bird*, *supra,* 5 Cal.5th at p. 540 [noting that *Barrett v. Rosenthal*, *supra,* 40 Cal.4th 33 voiced "qualms" that *Zeran*'s interpretation of section 230 provides blanket immunity for those who intentionally redistribute defamatory statements, but held "these concerns were of no legal consequence" where principles of statutory interpretation compelled a broad construction].) And while it is not this Court's role to judge the wisdom of the policy embodied by section 230, there are good reasons to support it. As the court in *Levitt v. Yelp! Inc.* (N.D. Cal., Oct. 26, 2011, No. C-10-1321 EMC) 2011 WL 5079526 reasoned,

> traditional editorial functions often include subjective judgments informed by political and financial considerations. [Citation.] Determining what motives are permissible and what are not could prove problematic. Indeed, from a policy perspective, permitting litigation and scrutin[izing] motive could result in the "death by ten thousand duck-bites" against which the Ninth Circuit cautioned in interpreting § 230(c)(1). [(*Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, *supra,* 521 F.3d at p. 1174.)]
>
> One of Congres[s]'s purposes in enacting § 230(c) was to avoid the chilling effect of imposing liability on providers by both safeguarding the "diversity of political discourse ... and myriad avenues for intellectual activity" on the one hand, and "remov[ing] disincentives for the development and utilization of blocking and filtering technologies" on the other hand. §§ 230(a), (b); *see also* S.Rep. No. 104–230, at 86 (1996) (Conf.Rep.), *available at* 1996 WL 54191, at *[194] (describing purpose of section 230 to protect providers from liability "for actions to restrict or to enable restrict[ion] of access to objectionable online material"). For that reason, "[C]lose cases ... must be resolved in favor of immunity, lest we cut the heart out of section 230 ...." [(*Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, *supra,* 521 F.3d at p. 1174.)]
>
> As illustrated by the case at bar, finding a bad faith exception to immunity under § 230(c)(1) could force Yelp to defend its editorial decisions in the future on a case by case basis and reveal how it decides what to publish and what not to publish. Such exposure could lead Yelp to resist filtering out false/unreliable reviews (as someone could claim an improper motive for its decision), or to immediately remove all negative reviews about which businesses complained (as failure to do so could expose Yelp to a business's claim that Yelp was

> strong-arming the business for advertising money). The Ninth Circuit has made it clear that the need to defend against a proliferation of lawsuits, regardless of whether the provider ultimately prevails, undermines the purpose of section 230.

(*Levitt v. Yelp! Inc.*, *supra,* 2011 WL 5079526, at *8-9.) In the Court's view, these concerns are particularly salient here, where the challenged services are by definition more curated than defendants' core service and could not exist without more robust screening by defendants.

In opposition to defendants' demurrer, Prager cites a number of cases that affirm the principle applied in *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, *supra,* 521 F.3d 1157, which held that a service provider is not entitled to CDA immunity with regard to content it develops itself. However, this principle is inapposite here. Prager does not allege that defendants developed any of Prager's content or appended any commentary to it—to the contrary, they allege the content became completely invisible in "Restricted Mode" or was simply demonetized. Applying CDA immunity under these circumstances does not conflict with *Roommates*. (See *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, *supra,* 521 F.3d at p. 1163 [in enacting CDA immunity, "Congress sought to immunize the *removal* of user-generated content, not the *creation* of content"].)[8]

Finally, Prager contends that applying CDA immunity here would constitute an unlawful prior restraint on its speech in violation of the First Amendment. However, a federal court has already held that defendants' conduct does not violate the First Amendment, and this Court agrees with that analysis for the reasons discussed in connection with its analysis of Prager's claim under the California Constitution. Moreover, Prager does not allege that defendants prevented it from engaging in speech, even on their own platform—again, it contends that certain videos were excluded from "Restricted Mode" and/or were demonetized.

The Court consequently finds that section 230(c)(2)(B) bars Prager's claims related to "Restricted Mode" and section 230(c)(1) bars all of its claims, with the possible exception of those based on its own promises and representations, which are discussed below.[9]

C. Breach of the Implied Covenant of Good Faith and Fair Dealing and Fraud Under the UCL

Finally, Prager correctly urges that some California authority holds section 230(c)(1) of the CDA does not apply to claims based on a defendant's own promises and representations to a plaintiff, rather than its role as a publisher. (See *Demetriades v. Yelp, Inc.* (2014) 228 Cal.App.4th 294, 313 [this immunity does not apply where "plaintiff seeks to hold Yelp liable for its own statements regarding the accuracy of its filter"]; but see *Hassell v. Bird*, *supra,* 5 Cal.5th at p. 542 [disapproving of "creative pleading" in an attempt to avoid section 230 immunity].) This authority does not apply to the Court's finding of immunity under section 230(c)(2)(B). In any event, Prager's claims asserting this type of theory—namely, its claim for

[8] Although it does not bring a claim for defamation, Prager appears to suggest that defendants have defamed it by removing its content from "Restricted Mode" or demonetizing it. Such a claim would likely be foreclosed by the ruling in *Bartholomew v. YouTube, LLC.* (2017) 17 Cal.App.5th 1217, 1234.

[9] The Court thus does not address defendants' argument that Prager's claims are barred by the First Amendment.

breach of the implied covenant of good faith and fair dealing and its claim under the fraud prong of the UCL—do not state a cause of action.

Prager does not and cannot state a claim for breach of the implied covenant of good faith and fair dealing in light of the express provisions of YouTube's Terms of Service, which provide that "YouTube reserves the right to remove Content without prior notice" and which also allow YouTube to "discontinue any aspect of the Service at any time." (See Declaration of Brian Willen, Ex. 1; *Song fi Inc. v. Google, Inc.* (N.D. Cal. 2015) 108 F.Supp.3d 876, 885 [plaintiff could not state a claim for violation of the covenant of good faith and fair dealing based on content removal in light of YouTube's Terms of Service].) Similarly, YouTube's AdSense Terms of Service reserve the right "to refuse or limit your access to the Services." (Declaration of Brian Willen, Ex. 8; see *Sweet v. Google Inc.* (N.D. Cal., Mar. 7, 2018, No. 17-CV-03953-EMC) 2018 WL 1184777, at *9-10 [plaintiff could not state a claim for violation of the covenant of good faith and fair dealing based on demonitization in light of similar reservation of rights in YouTube's Partner Program Terms].) "[C]ourts are not at liberty to imply a covenant directly at odds with a contract's express grant of discretionary power except in those relatively rare instances when reading the provision literally would, contrary to the parties' clear intention, result in an unenforceable, illusory agreement." (*Third Story Music, Inc. v. Waits* (1995) 41 Cal.App.4th 798, 808.) That is not the case here, and Prager does not contend that it is. (See *Sweet v. Google Inc.*, *supra,* 2018 WL 1184777, at *9-10 [applying *Third Story*].)

As to the UCL fraud claim, to the extent it is based on the "four essential freedoms" set forth above and similar statements, these statements are non-actionable puffery. (See *Demetriades v. Yelp, Inc.*, *supra,* 228 Cal.App.4th at p. 311 [" 'a statement that is quantifiable, that makes a claim as to the "specific or absolute characteristics of a product," may be an actionable statement of fact while a general, subjective claim about a product is non-actionable puffery,' " quoting *Newcal Industries, Inc. v. Ikon Office Solution* (9th Cir.2008) 513 F.3d 1038, 1053]; *Prager University v. Google LLC*, *supra,* 2018 WL 1471939, at *11 ["None of the statements about YouTube's viewpoint neutrality identified by Plaintiff resembles the kinds of 'quantifiable' statements about the 'specific or absolute characteristics of a product' that are actionable under the Lanham Act."].)

Prager also alleges that defendants represented that "the 'same standards apply equally to all' when it comes to the content regulation on YouTube." (FAC, ¶ 85; see also *id.* at ¶ 13.) While this statement is arguably more than mere puffing (see *Demetriades v. Yelp, Inc.*, *supra,* 228 Cal.App.4th at p. 311-312), Prager does not allege that it suffered a loss of money or property as a result of its reliance on this statement. "There are innumerable ways in which economic injury from unfair competition may be shown," including where a plaintiff "ha[s] a present or future property interest diminished." (*Kwikset Corp. v. Superior Court (Benson)* (2011) 51 Cal.4th 310, 323; see also *Alborzian v. JPMorgan Chase Bank, N.A.* (2015) 235 Cal.App.4th 29, 38 [UCL "unlawful" plaintiffs established standing by alleging diminished credit score caused by defendant's false negative reporting to credit agencies, even where they never made payments on the loan at issue].) The "lost income, reduced viewership, and damage to brand, reputation, and goodwill" that Prager alleges (FAC, ¶ 157) would certainly satisfy this requirement if there were a causal connection between Prager's alleged reliance on defendants' statement in participating in the YouTube service and these harms. However, these injuries cannot have resulted from Prager's decision to use YouTube: they could only have been caused by YouTube's later decisions to restrict and/or demonetize Prager's content.

(See *Prager University v. Google LLC*, *supra,* 2018 WL 1471939, at *11-12 ["Plaintiff has not sufficiently alleged that it 'has been or is likely to be injured as the result of the' statements about YouTube's viewpoint neutrality. [Citation.] As discussed above, any harm that Plaintiff suffered was caused by Defendants' decisions to limit access to some of Plaintiff's videos."].) These later decisions by YouTube could not have been relied on by Prager. (See *id.* at *11 ["Although Plaintiff asserts that it has suffered injury in the form of 'lower viewership, decreased ad revenue, a reduction in advertisers willing to purchase advertisements shown on Plaintiff's videos, diverted viewership, and damage to its brand, reputation and goodwill," … nothing in Plaintiff's complaint suggests that this harm flowed directly from Defendants' publication of their policies and guidelines. Instead, any harm that Plaintiff suffered was caused by Defendants' decisions to limit access to some of Plaintiff's videos …."].) Moreover, recognizing this theory would appear to conflict with principles of defamation law as recently discussed in *Bartholomew v. YouTube, LLC.* (2017) 17 Cal.App.5th 1217.

Prager thus fails to state a cause of action based on the implied covenant of good faith and fair dealing or the fraud prong of the UCL.

D. Conclusion and Order

For all these reasons, the demurrer to the first through fourth causes of action is SUSTAINED WITHOUT LEAVE TO AMEND.

III. Motion for Preliminary Injunction

As discussed above, Prager has not shown a reasonable probability of success on the merits in this action. Its motion for a preliminary injunction is consequently DENIED. (See *San Francisco Newspaper Printing Co. v. Superior Court (Miller)* (1985) 170 Cal.App.3d 438, 442.)

The Court will prepare the order.

- oo0oo -

CERTIFICATE OF SERVICE

I hereby certify that on October 28, 2019, I filed the foregoing Petition for Panel Rehearing and Rehearing En Banc with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Neal Kumar Katyal
Neal Kumar Katyal