No. 17-17351

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 (SAN JOSE)
DISTRICT COURT CASE NO. 5:17-CV-02915-EJD

APPELLANT'S OPENING BRIEF

TERRY BUDD
BUDD LAW PLLC
120 Lyndhurst Circle
Wexford, Pennsylvania 15090
(412) 613-2541

CHRISTOPHER M. VERDINI
ANNA SHABALOV
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, Pennsylvania 15222
(412) 355-6500

– and –

EDWARD P. SANGSTER
K&L GATES LLP
Four Embarcadero Center, Suite 1200
San Francisco, California 94111
(415) 882-8200

Attorneys for Plaintiff-Appellant

CORPORATE DISCLOSURE STATEMENT

Enigma Software Group USA, LLC is a Florida corporation with its principal place of business in Florida. Enigma Software Group USA, LLC is 100% owned by Globalist LLC, a Delaware limited liability company. Globalist LLC has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes:

I. INTRODUCTION

In 1996, when the Internet was a nascent technology, Congress responded to concerns about the exposure of children to the obscenity and pornography flooding the web by passing the Communications Decency Act ("CDA"). Section 230 of the CDA empowered providers of interactive computer services to block obscene and pornographic content themselves and incentivized them to provide tools that would enable parents to protect their children, by immunizing the providers against certain types of claims. *See Batzel v. Smith*, 333 F. 3d 1018, 1026 (9th Cir. 2003) ("The primary goal of the Act was to control the exposure of minors to indecent material."). Congress set forth particular policies that were central to the CDA's governance of the Internet: (1) promotion of the "continued development of … interactive computer services"; (2) preservation of "the vibrant and competitive free market"; (3) encouragement of technologies that "maximize user control over what information" they receive on the Internet; and (4) removal of "disincentives for the development and utilization of blocking and filtering technologies" that foster parental control over materials that their children access. 47 U.S.C. § 230(b).

To further those express policies, Congress created an immunity under Section 230(c)(2), entitled "Protection for 'Good Samaritan' blocking and screening of offensive material," which specifies that:

> No provider or user of an interactive computer service shall be held liable on account of--
>
> > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> >
> > (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[1]

47 U.S.C. § 230(c)(2). *See also Batzel*, 333 F. 3d at 1028 (Section 230(c) was enacted "to encourage interactive computer services and users of such services to self-police the Internet for obscenity and other offensive material, so as to aid parents in limiting their children's access to such material").

Twenty years later, Defendant-Appellee Malwarebytes Inc. ("Malwarebytes"), advanced a tortured and illogical interpretation of Section 230 in an attempt to shield itself from liability for unlawful predatory practices it employed against a direct competitor. In particular, Malwarebytes invoked Section 230 as immunizing its unilateral decision to designate and block as "otherwise objectionable" the legitimate anti-malware and computer optimization programs of Enigma Software Group USA, LLC ("ESG"). Malwarebytes did so based on the inherently nonsensical claim that ESG programs are "Potentially Unwanted

[1] Although the statutory text references "material described in paragraph (1)," this is "a typographical error, and … instead the reference should be to paragraph (A), i.e., § 230(c)(2)(A)." *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 n.5 (9th Cir. 2009).

Programs" ("PUPs") and "threats" to consumers who have, in fact, affirmatively chosen ESG programs, elected to download and install them, and contracted and paid for them. As alleged in ESG's First Amended Complaint ("FAC"), Malwarebytes affirmatively ***disables*** the operation of ESG programs such that consumers—both existing and potential ESG customers—who attempt to download, install, and use ESG programs, are blocked from doing so. Moreover, Malwarebytes provides only a confusing, labyrinthine, and unworkable method to bypass that block; many users simply cannot navigate the purported bypass, making a mockery of the "user control" at the core of Section 230.

Malwarebytes' conduct is not that of a Good Samaritan. It is the unlawful, predatory, and anti-competitive conduct of a direct competitor of ESG. Malwarebytes diverts ESG's customers, harms ESG's business, diminishes consumer choice, and leaves consumers more vulnerable to cyber attack. Malwarebytes' conduct is the equivalent of Apple programming its smartphones to disable competing Samsung smartphones whenever both are in the same household. In fact, by disabling ESG's programs so that they cannot run alongside Malwarebytes' on the same computer, Malwarebytes is opening the door to every computer security company in the market blocking and disabling the programs of its competitors. In such a world, interactive computer services providers would focus more on fighting each other than on combatting cyber threats. As a result, the variety and quality of products available to consumers would inevitably suffer. At a minimum, consumers would be able to run only one company's cybersecurity protection offerings on their computers and would be unable to follow the industry best practice of obtaining multiple layers of cybersecurity protection by simultaneously running multiple programs. This, in turn, would drastically increase the risks consumers face from fast-evolving cyber attacks, malware, hacking, and identity theft.

Yet Malwarebytes argued to the district court that the CDA allowed it to block a direct competitor simply because it deemed ESG programs "otherwise objectionable" under 47 U.S.C. § 230(c)(2)(A), without reference to any "independent standard" and without being subject to any obligation to act in good faith. E.R. 15.[2] In other words, Malwarebytes claims it can adopt its own subjective standard under Section 230 and need not explain, justify or answer for a standard specifically intended to harm a direct competitor and gain market share for reasons unrelated to the merits of their respective products. As the Honorable Raymond C. Fisher of the Ninth Circuit incisively foresaw years ago, such an interpretation would turn the intent of the CDA on its head:

> [A] blocking software provider might abuse [CDA] immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material "otherwise

[2] Citations to "E.R. __" refer to pages in ESG's Excerpts of Record, filed with this opening brief.

> objectionable." Focusing for the moment on anticompetitive blocking, I am concerned that blocking software providers who flout users' choices by blocking competitors' content could hide behind § 230(c)(2)(B) when the competitor seeks to recover damages. ***I doubt Congress intended § 230(c)(2)(B) to be so forgiving.***

Zango, 568 F.3d at 1178 (Fisher, J., concurring) (emphasis added).

The district court, in turn, adopted Malwarebytes' wrong-headed and unduly expansive argument, holding in effect that any provider of interactive computer services can block ***any material*** on the Internet for an anticompetitive purpose, in bad faith, or on a malicious whim—in short, ***for any reason***—as long as the provider claims the blocked material is "otherwise objectionable" under Section 230(c)(2). This erroneous holding would have a far-reaching negative impact on cybersecurity, the free market, consumer choice and the free exchange of ideas. As a leading voice on Internet law and consumer protection, this Court is uniquely positioned to protect consumers from these unjustified—and dangerous—consequences, by reversing the district court's erroneous statutory interpretation and its dismissal of ESG's claims.

II. STATEMENT OF JURISDICTION

The district court had subject matter jurisdiction under 28 U.S.C. §§ 1331, 1332, 1338, and 1367. Federal question jurisdiction existed over ESG's claims arising under the Lanham Act, 15 U.S.C. § 1051 *et seq*. ESG's state law claims were subject to supplemental jurisdiction. Additionally, diversity jurisdiction existed because ESG is a citizen of Florida, Malwarebytes is a citizen of Delaware and California, and the amount in controversy exceeds $75,000.

This Court has jurisdiction pursuant to 28 U.S.C. § 1291, because the district court's entry of judgment is an appealable final decision. The district court issued its order dismissing ESG's claims and entered judgment in favor of Malwarebytes on November 7, 2017. ESG timely filed a Notice of Appeal on November 21, 2017. *See* Fed. R. App. P. 4(a)(1)(A) (Notice of Appeal to be filed "within thirty days after entry of the judgment or order appealed from").

III. STATEMENT OF ISSUES PRESENTED FOR REVIEW

1. Did the district court err in holding that CDA Section 230(c)(2) immunizes Malwarebytes' anti-competitive behavior when that behavior conflicts with the Congressional policies Section 230 is intended to effectuate?

2. Did the district court err in holding that CDA Section 230(c)(2)(A) imposes no objective standard on the definition of "otherwise objectionable" material, such that Malwarebytes can be immune under Section 230(c) when it unilaterally declares ESG programs to be "potentially unwanted" and thus "otherwise objectionable"?

3. Did the district court err in holding that Malwarebytes' behavior falls under CDA Section 230(c)(2)(B), when Malwarebytes does not simply "enable" or "make available" the "technical means to restrict access to material" described in

Section 230(c)(2)(A), but instead unilaterally blocks ESG programs that users affirmatively choose to download, install, use, and purchase?

4. Did the district court err in holding that CDA Section 230(c)(2)(B) contains no good faith requirement, such that Malwarebytes may be immune for action taken in bad faith "to enable or make available…the technical means to restrict access to material" described in Section 230(c)(2)(A)?

5. Did the district court err in holding that ESG's Lanham Act claim was subject to Section 230(c) immunity, when CDA Section 230(e)(2) provides that "nothing in [Section 230] shall be construed to limit or expand any law pertaining to intellectual property"?

6. Should the district court's dismissal of ESG's claims be reversed?

IV. APPLICABLE STATUTE

<u>47 U.S.C. § 230</u>

§ 230. Protection for private blocking and screening of offensive material

(a) Findings

The Congress finds the following:

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

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

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

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

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

(b) Policy

It is the policy of the United States--

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

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

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

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

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

(1) Treatment of publisher or speaker

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

(2) Civil liability

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

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

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

(d) Obligations of interactive computer service

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

(e) Effect on other laws

(1) No effect on criminal law

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

(2) No effect on intellectual property law

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

(3) State law

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

(4) No effect on communications privacy law

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

(f) Definitions

As used in this section:

(1) Internet

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

(2) Interactive computer service

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

(3) Information content provider

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

(4) Access software provider

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

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

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

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

V. STATEMENT OF THE CASE

A. Allegations in the First Amended Complaint.

ESG and Malwarebytes are direct competitors in the anti-malware and computer security market. E.R. 23 at ¶¶ 3-4; E.R. 34 at ¶ 54.

ESG is an established computer security company whose consumer security protection anti-malware flagship product SpyHunter 4 has protected millions of users from malware, system breaches, and identity theft. *See* E.R. 22 at ¶ 1; E.R. 33 at ¶ 45. SpyHunter 4 and ESG's advanced Windows optimization and registry cleaner, RegHunter, which provides multiple functionalities, including tools for data privacy protection, have received top industry certifications. E.R. 33 at ¶¶ 46-47; E.R. 34 at ¶ 52.

Malwarebytes' flagship product, MBAM, competes directly with SpyHunter 4. E.R. 23 at ¶ 4; E.R. 34 at ¶ 54. Through Malwarebytes' website, consumers can download free versions of MBAM and Malwarebytes' anti-adware product, AdwCleaner. E.R. 35 at ¶ 58. Malwarebytes also offers a "Premium" MBAM product that consumers must purchase after a free 14 day-trial to retain full-product functionality. *Id.* at ¶¶ 58-59.

Malwarebytes also markets and promotes its MBAM product through an affiliate program, whereby it pays its affiliates commissions for purchases of MBAM through the affiliates' websites. Bleeping Computer LLC ("Bleeping") is a Malwarebytes affiliate. E.R. 27 at ¶ 22. On January 5, 2016, ESG filed suit against Bleeping in the United States District Court for the Southern District of New York, seeking redress for Bleeping's deliberate dissemination of false and misleading information about ESG and SpyHunter 4 (the "Related Case"). *Id.* at ¶ 23; E.R. 35 at ¶ 61. Bleeping instructed consumers not to install, or to uninstall, SpyHunter and instead purchase MBAM. *Id*. Malwarebytes directly profited from Bleeping's unlawful conduct. In fact, it funded a portion of Bleeping's defense costs in the Related Case. E.R. 36 at ¶¶ 62, 64.

In the Related Case, ESG served Malwarebytes with a subpoena seeking documents reflecting Malwarebytes' relationship with Bleeping and its collaboration with Bleeping's efforts to divert sales from ESG to Malwarebytes (the "Subpoena"). E.R. 27 at ¶ 24; E.R. 36 at ¶ 66. Less than a week before Malwarebytes' response to the Subpoena was due, Malwarebytes—facing the prospect of having to produce documents and testify under oath regarding its involvement in Bleeping's anti-competitive conduct and risking the loss of the competitive advantages that Bleeping's campaign provided—began to characterize ESG programs as PUPs and "threats" to their users. E.R. 27-28 at ¶ 25; E.R. 37-38 at ¶¶ 72-73. Simultaneously, Malwarebytes publicly announced that it had amended the characteristics it used to define PUPs to include "obtrusive, misleading, or deceptive advertising, branding, or search practices," "diminishe[d] user experience," "predominantly negative feedback or ratings from the user community," and other factors that largely tracked Bleeping's allegations about ESG in the Related Case. E.R. 24 at ¶ 7; E.R. 27-28 at ¶¶ 21, 25-27; E.R. 36-38 at ¶¶ 67, 71-73.

Then, having characterized ESG's SpyHunter and RegHunter as "potentially unwanted," Malwarebytes products began to block ESG's consumers' actual installation and use of ESG products. E.R. 24-26 at ¶¶ 9, 16; E.R. 39 at ¶ 81. For consumers who had already installed and paid for ESG programs, MBAM "quarantined" ESG program files as PUPs in a "Total Threats Detected" window, preselected the files for removal, and prompted the user to remove them via a "Remove Selected" button. E.R. 40-42 at ¶¶ 82-84. Regardless of whether the user clicked "Remove Selected," MBAM prevented the launch of ESG programs. *Id.* at ¶ 85. Moreover, even if the user attempted to "Restore" ESG programs from MBAM's "Quarantine," the user's subsequent attempt to launch ESG programs would again result in automatic quarantine and failure to launch. E.R. 24-26 at ¶¶ 10, 17; E.R. 43 at ¶¶ 86-89.

For consumers who attempted to download ESG products, MBAM blocked the installer files and prevented the download. E.R. 44 at ¶ 92. Even if a user knew that he or she could "Restore" the quarantined installer files, any subsequent attempt to download ESG programs would result in the same PUP warning and quarantine process. E.R. 25 at ¶ 11; E.R. 45 at ¶¶ 93-95. As a result, MBAM traps ESG users in a frustrating and unproductive cycle of attempting to restore or re-download ESG programs only to have the installer file blocked each and every time. E.R. 45 at ¶ 95. The only way a user can stop this cycle is to add the ESG files as "Malware Exclusions" within MBAM, a step that is wholly counterintuitive because neither ESG products nor PUPs (however defined) are malware. E.R. 44 at ¶¶ 90-91. And, even if a user knew how to do this, MBAM would continue to characterize and quarantine other ESG files as PUPs and "threats." *Id*.

In addressing the foregoing ESG allegations in its district court briefing, Malwarebytes suggested that it was easy for consumers to "whitelist" ESG programs within Malwarebytes' software and render them functional. *See, e.g.*, E.R. 14, 19. Malwarebytes' assertions are entirely inaccurate, as the numerous consumer complaints cited in the FAC demonstrate. *See* E.R. 47-53 at ¶¶ 101-23. In all events, however, its contentions raised a factual dispute that must be resolved in ESG's favor at the motion to dismiss stage.

To be clear, Malwarebytes does not simply provide consumers with a cautionary list or review of programs that Malwarebytes looks upon unfavorably, as Consumer Reports might do. Rather, Malwarebytes' programmers purposefully act to electronically disable, *i.e.* render unusable, ESG programs that, in many cases, a consumer has already purchased and paid for. In effect, Malwarebytes characterizes ESG products as "potentially unwanted"; having done so, Malwarebytes disrupts and disabling an ESG customer's actual choice of the computer software the consumer wants to use.

Malwarebytes knows that ESG programs are legitimate, pose no security threat to a user's computer, and are not harassing in any way. E.R. 53 at ¶¶ 124-25. Malwarebytes has no objective, good faith basis to claim that ESG programs—that consumers have chosen to download and purchase—are "potentially unwanted." E.R. 26 at ¶ 18; E.R. 54 at ¶¶ 126-27. No such basis exists. *Id.* Malwarebytes' "revision" of its PUP criteria is a mere pretense under which it blocks user access to ESG programs, gains an unfair business advantage, furthers its anticompetitive scheme, and retaliates against ESG for its conduct in the Related Case. E.R. 24 at ¶¶ 7-8; E.R. 27-28 at ¶¶ 21, 25-27; E.R. 36-38 at ¶¶ 67, 72-73, 76; E.R. 54 at ¶ 127. Indeed, a Malwarebytes employee (and developer of AdwCleaner, a product acquired by Malwarebytes shortly after it announced its revised PUP criteria) clarified the targeted nature of Malwarebytes' attack in an tweet that called out ESG: "#AdwCleaner by @Malwarebytes now fully detects and removes #SpyHunter from Enigma Software Group #PUP." E.R. 39 at ¶ 78.

By characterizing ESG programs as "potentially unwanted," and blocking their use by consumers who have purchased those programs, Malwarebytes is falsely representing to the consuming public that ESG programs, including SpyHunter 4 which competes directly with MBAM, are "threats" that will compromise computer security if they are downloaded and/or not removed. E.R. 25 at ¶ 15. Before ESG filed its FAC, ESG had already received more than 300 consumer complaints about Malwarebytes' interference with their ESG programs. E.R. 47 at ¶ 101; E.R. 53 at ¶ 123. Some consumers reported that, even though they wanted to use ESG programs, they found it impossible or too difficult to exclude them from Malwarebytes' block and were, therefore, canceling their ESG accounts, not renewing their subscriptions, and/or requesting refunds of their subscription fees. E.R. 47-54 at ¶¶ 101-23, 132. ESG's sales of SpyHunter 4 and RegHunter licenses have already declined. They will continue to do so if Malwarebytes' unlawful and predatory anti-competitive conduct is allowed to continue. E.R. 54 at ¶ 131.

B. Procedural Background.

ESG filed this case in the Southern District of New York. *See* E.R. 125 at Dkt. 1. Malwarebytes moved to dismiss the FAC for lack of personal jurisdiction and failure to state a claim under Rules 12(b)(2) and 12(b)(6) of the Federal Rules of Civil Procedure, and, in the alternative, to transfer the case to the Northern District of California under 28 U.S.C. § 1404. *See* E.R. 127-28 at Dkt. 17-22. Pursuant to a court order permitting the filing of an amended complaint in response to a motion to dismiss, ESG filed its FAC. *See* E.R. 128-29 at Dkt. 24, 33. Malwarebytes then renewed its motion to dismiss or transfer. *See* E.R. 130 at Dkt. 37-42. The Court granted only the § 1404 motion to transfer for convenience and expressly declined to reach the motion to dismiss. E.R. 134 at Dkt. 67.

Upon transfer, Malwarebytes renewed its Rule 12(b)(6) motion to dismiss ("Motion"), arguing that ESG had failed to state a claim for four separate reasons: (1) Malwarebytes was immune from all of ESG's claims under Section 230(c)(2) of the CDA; (2) ESG had failed to allege that Malwarebytes made actionable "false and misleading statements" under the Lanham Act or New York General Business Law Section 349; (3) ESG had failed to allege that Malwarebytes' statements were made in "commercial advertising or promotion" as required by the Lanham Act; and (4) ESG had not sufficiently plead its tortious interference claims. *See* E.R. 138 at Dkt. 97. ESG filed an Opposition to the Motion and Malwarebytes filed a Reply in support of its Motion. *See id.* at Dkt. 100, 102.

Without hearing oral argument, the district court issued its Order dated November 7, 2017, granting Malwarebytes' Motion and dismissing ESG's FAC with prejudice. E.R. 2-8; *see also* E.R. 1 (entering final judgment in favor of Malwarebytes). The district court's sole ground for dismissal was Malwarebytes' purported immunity under CDA Section 230(c)(2)(B). E.R. 8. Specifically, the court adopted Malwarebytes' erroneous argument that *Zango v. Kaspersky*, 568

F.3d 1169, was dispositive and permitted a provider of interactive computer services to unilaterally deem any content "objectionable." E.R. 5-6. In so reasoning, the court incorrectly concluded that *Zango* and this case were "factually indistinguishable" because Malwarebytes supposedly had determined that ESG programs were "malware," the category of material blocked in *Zango*. E.R. 6. ESG, however, expressly pled—and Malwarebytes expressly admitted—that Malwarebytes had characterized and blocked ESG programs as "potentially unwanted programs," ***not malware***. E.R. 24 at ¶¶ 7, 9; E.R. 38-39 at ¶¶ 73-76, 80-81. The court further agreed with Malwarebytes' implausible claim that Section 230(c)(2)(B) does not require an entity to act in "good faith" when it enables or makes available to others "the technical means to restrict access to material described in" Section 230(c)(2)(A). E.R. 6-7. Finally, the court held that ESG's Lanham Act claim was not exempt from Section 230's grant of immunity, finding that the claim is not an "intellectual property claim." E.R. 7-8. The court did not reach Malwarebytes' remaining arguments as to the adequacy of ESG's pleading. ESG timely appealed the court's erroneous interpretation of CDA Section 230(c)(2), its misapplication of the motion to dismiss standard, and its dismissal of the FAC.

VI. SUMMARY OF ARGUMENT

1. Malwarebytes' behavior, and the district court's interpretation of CDA Section 230(c), which would provide immunity to any user or provider of interactive computer services blocking any content for any reason, fly in the face of each of Section 230's stated policies. including (1) the promotion of the "continued development of … interactive computer services"; (2) the preservation of "the vibrant and competitive free market"; (3) the encouragement of "the development of technologies which maximize user control"; and (4) the protection of children from obscene content online. 47 U.S.C. § 230(b).

2. The district court erred in holding that the meaning of "otherwise objectionable" in Section 230(c)(2)(A)'s definition of offensive material as "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" has no objective content. Fundamental tenets of statutory construction—*ejusdem generis* and the rule against superfluity—dictate that a catch-all term like "otherwise objectionable" at the end of a list designating specific categories must be limited by the preceding words, to avoid rendering those words superfluous. Pursuant to these principles, "otherwise objectionable" material must be akin to "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing" material. ESG programs are not, and thus Malwarebytes is not immune from liability for blocking them.

3. Malwarebytes' actions cannot be immunized because they fall outside the express terms of Section 230(c)(2)(B), which provides immunity only to actions "taken to enable or make available to … others the technical means to restrict access" to the material defined in sub-section (c)(2)(A). Rather than provide to others "the technical means to restrict access" to materials, Malwarebytes unilaterally blocks user access to ESG programs, which users have indicated they want, and thereby usurps consumer choice and user control.

4. The district court erred in holding that Section 230(c)(2)(B) contains no good faith requirement, because a harmonious reading of Section 230(c) renders good faith a necessary requirement in sub-section (c)(2)(B). Section 230(c) is captioned "Protection for '***Good Samaritan***' blocking and screening of offensive material" (emphasis added), and it defies logic that Congress intended to extend "Good Samaritan" immunity to entities acting in bad faith, as Malwarebytes has. Because ESG has adequately pled that Malwarebytes acted in bad faith, Malwarebytes is not entitled to Section 230(c)(2) immunity.

5. Even if Malwarebytes were immune under Section 230(c), that immunity does not extend to ESG's Lanham Act claim. Section 230 expressly provides that "nothing in [Section 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). The Lanham Act

is a "law pertaining to intellectual property," so even if Malwarebytes has CDA immunity, ESG's Lanham Act claim survives.

VII. STANDARD OF REVIEW

This Court reviews de novo a district court's dismissal of a complaint for failure to state a claim. *See Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1142 (9th Cir. 2008). "All allegations of material fact are taken as true and are construed in the light most favorable to" the nonmoving party. *Coalition For ICANN Transparency, Inc. v. VeriSign, Inc.*, 611 F.3d 495, 501 (9th Cir. 2010). A motion to dismiss must be denied "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009). Accordingly, a complaint need only allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This Court also reviews de novo questions of statutory interpretation. *Doe v. Internet Brands*, Inc., 824 F.3d 846, 850 (9th Cir. 2016).

VIII. ARGUMENT

A. ESG Pled Viable Claims As to Malwarebytes' Wrongful Anti-Competitive Campaign, Which the Court Did Not Reach.

In its FAC, on the basis of robust factual allegations regarding Malwarebytes' concerted anti-competitive campaign, ESG sought redress for Malwarebytes' (1) false advertising in violation of Lanham Act § 43(a), 15 U.S.C. § 1125(a); (2) use of deceptive acts and practices in violation of Section 349 of New York's General Business Law; (3) tortious interference with ESG's contractual relations with its customers; and (4) tortious interference with ESG's business relations with potential customers.

Specifically, in support of its Lanham Act false advertising claim, ESG alleged that (a) Malwarebytes' characterization of ESG products as PUPs and "threats" on its websites and in its programs are false statements made to advertise Malwarebytes' competing products; (b) that characterization is material in the cybersecurity market and thus likely to deceive relevant consumers as to the nature, quality and efficacy of ESG products; and (c) ESG has suffered the loss of existing and prospective customers and reputational damage as a result. *See* E.R. 55-56 at ¶¶ 134-43; *see also Skydive Ariz., Inc. v. Quattrocchi*, 673 F.3d 1105, 1110 (9th Cir. 2012) (elements of claim are "(1) a false statement of fact by the defendant in a commercial advertisement about … another's product; (2) the statement actually deceived or has the tendency to deceive a substantial segment of its audience; (3) the deception is material, in that it is likely to influence the purchasing decision; (4) the defendant caused its false statement to enter interstate commerce; and (5) the plaintiff has been or is likely to be injured as a result of the false statement…”). In support of its Section 349 claim, ESG alleged that Malwarebytes materially misled consumers by wrongly characterizing and blocking ESG products as PUPs and “threats,” and thereby harmed ESG through loss of sales and a lessening of goodwill. *See* E.R. 56-57 at ¶¶ 144-50; *see also Crawford v. Franklin Credit Mgmt. Corp.*, 758 F.3d 473, 490 (2d Cir. 2014) (elements of claim are “[1] that the challenged act or practice was consumer-oriented; [2] that it was misleading in a material way; and [3] that the plaintiff suffered injury as a result of the deceptive act”).

Finally, in support of its tortious interference claims, ESG alleged that (a) it had, and Malwarebytes knew about, contracts with existing customers and business relationships with prospective customers seeking to download, install, and use ESG programs; (b) Malwarebytes intentionally interfered with those relationships for wrongful, anticompetitive purposes by blocking that download, installation, and use, causing existing customers to terminate contracts early and seek refunds and prospective and existing customers to decline to do business with ESG; and (c) ESG consequently has been damaged by lost sales. *See* E.R. 57-58 at ¶¶ 151-68; *see also Kirch v. Liberty Media Corp.*, 449 F.3d 388, 400 (2d Cir. 2006) (elements of tortious interference with prospective economic advantage are "(1) [plaintiff] had a business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship"); *id.* at 401 (elements of tortious interference with contractual relations are "(1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of the contract; (3) the defendant's intentional procurement of the third-party's breach of the contract without justification; (4) actual breach of the contract; and (5) damages").

The district court dismissed the FAC without reaching the merits of ESG's substantive claims, because it erroneously held, as a threshold matter, that *Zango*'s interpretation of Section 230 rendered Malwarebytes immune from all of ESG's claims. E.R. 5-6.

B. The Ninth Circuit Has Not Decided the Section 230 Issues Presented Here.

In deciding *Zango* was dispositive, the district court accepted Malwarebytes' argument that the Ninth Circuit has already squarely decided the critical issues presented in this case. Specifically, the district court held that *Zango* purportedly gave a provider of interactive computer services "discretion" to "select the criteria it would use to identify objectionable computer programs." E.R. 6; *see also* E.R.

15 (arguing that *Zango* allowed a provider to "deem" a competitor's software somehow "objectionable" under § 230(c)(2), completely unmoored from any "independent standard").

The Ninth Circuit, however, did not, and could not, reach that issue in *Zango*, nor has it reached it in any other case. The *Zango* plaintiff ***waived*** any argument on appeal that its "software is not 'otherwise objectionable' under § 230(c)(2)." 568 F.3d at 1178 (Fisher, J., concurring). As a result, this Court specifically observed that "[b]ecause Zango has not argued that the statute limits the material a provider of an interactive computer service may properly consider 'objectionable,' that question is not before us." *Id.* at 1177 n.8. Thus, *Zango* did not hold that Section 230(c)(2) incorporates no independent standard for "otherwise objectionable" material. To the contrary, it expressly disclaimed any such holding. *Zango* likewise did not address whether Section 230(c)(2)(B) contains an implicit good faith requirement, as ESG argues here, nor has the Ninth Circuit reached that issue in any other case.

To the extent the arguments at issue here were addressed in *Zango* at all, it was in Judge Fisher's concurring opinion, which specifically noted that attention needs to be paid to the scope of Section 230 immunity to ensure it is not misused for anti-competitive purposes. *Id.* at 1178-80. Indeed, Judge Fischer observed that "[u]nless § 230(c)(2)(B) imposes some good faith limitation on what a blocking software provider can consider 'otherwise objectionable,' or some requirement that blocking be consistent with user choice, immunity might stretch to cover conduct Congress very likely did not intend to immunize." *Id*. at 1179. The anti-competitive concerns Judge Fisher highlighted are squarely presented by this case. Accordingly, this Court has, for the first time, the opportunity to construe Section 230, including its embedded statutory purposes, to address the precise scenario of which Judge Fisher warned, where a software provider "block[s] content for anticompetitive purposes or merely at its malicious whim." *Id.* at 1178.

C. Malwarebytes' Conduct Conflicts with the Statutory Policies Embedded in Section 230 and Should Not Be Immunized.

Malwarebytes' actions here conflict with the Congressional policies set forth in Section 230. The district court's determination that Malwarebytes' conduct was immunized under the CDA, therefore, was in error.

Section 230 sets forth express Congressional policies the CDA is intended to effectuate:

> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
>
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

47 U.S.C. § 230(b). The district court's construction of Section 230 and its extension of the statutory immunity provided under Section 230(c) to Malwarebytes' actions run afoul of each of these policies and the fundamental purposes of the CDA. *See Collins v. Gee W. Seattle LLC*, 631 F.3d 1001, 1005 (9th Cir. 2011) ("[W]e may not read a statute's plain language to 'produce a result contrary to the statute's purpose or lead to unreasonable results.'" (quoting *U.S. v. Combs*, 379 F.3d 564, 569 (9th Cir. 2004)); *cf. Hernandez v. Williams, Zinman & Parham PC*, 829 F.3d 1068, 1073 (9th Cir. 2016) ("The words of a statute are, of course, dead weights unless animated by the purpose of the statute.").

1. The Court's Extension of Immunity to Malwarebytes Conflicts with the CDA's Policies of Promoting Innovation, Free Markets, and Consumer Choice.

The district court's statutory construction immunizes blatantly anticompetitive behavior. In doing so, it fails to further the first three interrelated Section 230 policies expressly stated by Congress.

First, the construction does not promote, but rather discourages, "the continued development of the Internet and other interactive computer services."

47 U.S.C. § 230(b)(1). Indeed, it would permit a direct competitor to interfere with ESG's efforts to develop quality computer security and optimization programs that protect vulnerable users and their data privacy against a fast-developing array of cyber threats.

Second, the construction does not preserve, but rather erodes, "the vibrant and competitive free market." 47 U.S.C. § 230(b)(2). It would allow a company that is dissatisfied with its track record in the free market to quarantine, disable and block a competitor's programs, rather than compete on the merits, thereby substantially diminishing consumer choice. In this case, Malwarebytes can block access to ESG products by consumers who have already affirmatively indicated they want to purchase those products. Malwarebytes' behavior violates the core purposes of a competitive free market: it leaves consumers with fewer product choices, lower quality services, and higher prices. *See Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of U. of Okla.*, 468 U.S. 85, 106-07 (1984) ("The anticompetitive consequences of this arrangement are apparent. Individual competitors lose their freedom to compete. … Price is higher and output lower than they would otherwise be, and both are unresponsive to consumer preference."); *U.S. v. Syufy Enters.*, 903 F.2d 659, 663 (9th Cir. 1990) ("When competition is impaired, producers may be able to reap monopoly profits, denying consumers many of the benefits of a free market.").

A construction of Section 230 that permits such anti-competitive behavior is antithetical to the key tenets of our economic system. *See Nat'l Soc. of Prof. Engineers v. U. S.*, 435 U.S. 679, 695 (1978) ("[U]ltimately competition will produce not only lower prices, but also better goods and services. The heart of our national economic policy long has been faith in the value of competition. … The assumption that competition is the best method of allocating resources in a free market recognizes that all elements of a bargain-quality, service, safety, and durability-and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers." (internal quotations and citation omitted)); *Syufy*, 903 F.2d at 662-63 ("Competition is the driving force behind our free enterprise system. … If, as the metaphor goes, a market economy is governed by an invisible hand, competition is surely the brass knuckles by which it enforces its decisions.").

Finally, a construction of Section 230 that would immunize Malwarebytes' behavior does not encourage, but rather inhibits, "the development of technologies which maximize user control." 47 U.S.C. § 230(b)(3). Malwarebytes has instituted a block that (1) provides no explanation to users of what is objectionable about ESG's programs or for what reasons they are "potentially unwanted"; (2) includes ESG's programs in an undifferentiated, and sometimes extremely long, list of malware and threats "detected" on a computer, all of which are pre-selected for deletion; and (3) many users find extremely difficult, or impossible, to opt-out of. This block restricts user control and prevents consumers from utilizing their own preferred combination of anti-malware software. If Malwarebytes' block of ESG programs were actually intended to promote user control, Malwarebytes (1) would not pre-select ESG programs for deletion; (2) would provide users with increased transparency about why it characterizes ESG programs as PUPs and blocks them; and (3) would provide a clear, easy-to-use opt-out method. Malwarebytes does none of these.

If each anti-malware software provider behaved as Malwarebytes has, blocking access to its competitors' products, consumers would be able to run only a single anti-malware program on their computer at a time. As a result, they would be reliant on a single software provider's threat database and far more vulnerable to cyber attacks than if they were able to layer protections from multiple programs, as cybersecurity best practices dictate. And the immunization of such behavior would have serious implications well beyond the context of competing computer security software providers. It could, for instance, protect an individual ideologically opposed to the vaccination of children who distributes a software program that blocks users' access to legitimate medical information online, including vaccine research in online medical journals for which doctors have paid subscription fees and vaccination records and medical test results posted on a health care provider's online patient services portal. Under Malwarebytes' theory, the individual would not even need to disclose to users the basis for the block, but could simply report medical websites users attempt to access as generalized "threats."

Ultimately, by blocking ESG customers from using the ESG programs they have chosen on the specious ground that those programs are "potentially unwanted," Malwarebytes is taking the nonsensical position that it can bar consumers' access to programs they have selected. Thus, Malwarebytes' construction of Section 230 effectively repudiates both consumer choice and user control.

The law would not countenance Apple programming its iPhones to disable and render inoperative any Samsung smartphones within a set radius solely to gain market share from Samsung. Such anticompetitive behavior would plainly interfere with Samsung's right to fair competition and consumers' rights to free choice of provider and to the use of products and services for which they have paid. Yet the district court's holding—unmoored as it is from the free market and consumer choice policies of the CDA—would allow equivalent behavior simply because it occurs on the Internet. This Court, however, has specifically cautioned that companies distributing goods over the Internet should not enjoy special privileges under the CDA:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1164 n.15 (9th Cir. 2008). Given the Congressional policies set forth in Section 230(b), no reason exists to immunize Malwarebytes' behavior solely because it takes place on the Internet rather than on the streets or in peoples' homes. "The Communications Decency Act was not meant to create a lawless no-man's-land on the Internet." *Id.* at 1164.

2. The Court's Extension of Immunity to Malwarebytes Does Not Advance the Statutory Purpose of Restricting Access to Indecent Materials.

The district court's statutory construction is also at odds with another stated policy of Section 230—the protection of children from exposure to pornographic and obscene material. Section 230(b)(4) of the ***Communications Decency*** Act, seeks to "remove disincentives" to the development of "blocking and filtering technologies" that would "empower parents to restrict their children's access to objectionable or inappropriate online material"; sub-section (b)(5) seeks to "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." 47 U.S.C. § 230(b)(4)-(5); *see also Zango*, 568 F.3d at 1173 ("The CDA was enacted to control the exposure of minors to indecent material on the Internet." (quotation omitted)). These statutory policies render illogical the extension of immunity to Malwarebytes and its efforts to impede access to ESG products—which bear no relationship to obscene materials and to the contrary address, *inter alia*, computer vulnerabilities that can serve as entry points for malware that originates from obscene materials or attacks computers with obscene materials. Indeed, "Section 230 is captioned 'Protection for 'Good Samaritan' blocking and screening of *offensive* material,' yet another indication that Congress was focused on potentially offensive materials, not simply any materials undesirable to a content provider or user." *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883 (N.D. Cal. 2015) (alteration in original). That is especially the case where, as here, Malwarebytes is seeking to block a direct competitor from developing and selling "blocking and filtering technologies." Far from "remov[ing] disincentives" to such developments—the express policy the CDA seeks to foster—Malwarebytes' conduct creates such "disincentives" as it seeks to inhibit the business of its competitor, ESG. Allowing, let alone immunizing, such conduct subverts the CDA's policies and purposes.

D. The Court's Extension of Immunity to Malwarebytes Has No Basis in the Substantive Provisions of Section 230(c)(2).

As demonstrated above, Malwarebytes' conduct undercuts, rather than advances, the congressionally-stated policies of Section 230. Moreover, the conduct is at odds with Section 230's substantive purposes—the protection of Internet users, and particularly children, from obscene and offensive materials. Malwarebytes' attempts to justify—and immunize—its conduct by labeling ESG's technology as "otherwise objectionable" under Section 230(c)(2)(A) and by shoehorning its conduct into the terms of Section 230(c)(2)(B) have no basis. Malwarebytes' efforts also ignore settled canons of statutory construction, the precise terms of sub-section (c)(2)(B) and the good faith requirement implicit in its argument for immunity.

1. ESG's Products Cannot be Characterized As "Otherwise Objectionable" Within the Meaning of Section 230(c)(2)(A).

Section 230(c) of the CDA expressly states that its "Good Samaritan" immunity protects the blocking and screening of "offensive material," defined in sub-section (A) as materials considered to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c)(2)(A). In its Order, the district court entirely ignored the first seven words which define materials subject to the statute and embraced an open-ended reading of "otherwise objectionable." E.R. 5-6. That reading ignored the tenets of *ejusdem* *generis* and the rule against superfluity. Moreover, "the ordinary meaning of 'otherwise objectionable,' as well as the context, history, and purpose of the Communications Decency Act all counsel against reading 'otherwise objectionable' to mean anything to which a content provider objects regardless of why it is objectionable." *Song fi*, 108 F. Supp. 3d at 884.

Ejusdem generis—"of the same kind"—dictates that "[w]here [as here] general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Cir. City Stores, Inc. v. Adams*, 532 U.S. 105, 114-15 (2001) (holding that the phrase "any ***other class*** of workers engaged in … commerce" is limited by preceding references to "seamen" and "railroad employees" (emphasis added)); *see also Yates v. U.S.*, 135 S. Ct. 1074, 1087 (2015) ("Had Congress intended 'tangible object' in § 1519 [which refers to 'any record, document, or tangible object'] to be interpreted so generically as to capture physical objects as dissimilar as documents and fish, Congress would have had no reason to refer specifically to 'record' or 'document.'"); *Guam Indus. Servs., Inc. v. Zurich Am. Ins. Co.*, 787 F.3d 1001, 1006 (9th Cir. 2015) ("It is ... a familiar canon of statutory construction that [catchall] clauses are to be read as bringing within a statute categories similar in type to those specifically enumerated." (quoting *Paroline v. U.S.*, 134 S.Ct. 1710, 1721 (2014) (alteration in original)));

Berns v. Sentry Select Ins. Co., 656 Fed. Appx. 326, 327 (9th Cir. 2016) (unpublished) ("[T]he term 'intentional' follows four more specific words ('dishonest,' 'malicious,' 'fraudulent,' and 'criminal') that describe particularly blameworthy conduct. The term 'intentional' should be read in light of these terms and therefore should be read as requiring some sort of wrongful conduct, not just any purposeful act.").

In addition, the rule against superfluity dictates that courts "give effect, if possible, to every clause and word of a statute." *Williams v. Taylor*, 529 U.S. 362, 404 (2000); *see also CSX Transp., Inc. v. Ala. Dept. of Revenue*, 562 U.S. 277, 295 (2011) ("We typically use ejusdem generis to ensure that a general word will not render specific words meaningless."). Thus, each word in a list—here, for example, "obscene" and "lewd"—that precedes a 'catch-all' term must have meaning. *See Yates*, 135 S. Ct. at 1087 ("The Government's unbounded reading of 'tangible object' would render those words misleading surplusage."); *Cir. City Stores*, 532 U.S. at 114 ("[T]here would be no need for Congress to use the phrases 'seamen' and 'railroad employees' if those same classes of workers were subsumed within the meaning of the … residual clause."); *Hibbs v. Winn*, 542 U.S. 88, 101 (2004) ("If … the term 'assessment,' by itself, signified '[t]he entire plan or scheme fixed upon for charging or taxing,' … the TIA would not need the words 'levy' or 'collection'; the term 'assessment,' alone, would do all the necessary work.”); *U.S. v. Thomsen*, 830 F.3d 1049, 1062 (9th Cir. 2016) (“The government's argument that § 1546(a) applies to more than immigration-related documents might be more persuasive if § 1546(a) referred simply to ‘document[s],’ rather than to ‘other documents’ … Here, the use of ‘other’ plainly suggests that the ‘document[s]’ are documents like the ones preceding them in the list, that is, immigration-related documents.”).

In construing the scope of immunity conferred by Section 230(c), courts, including the Northern District of California, have repeatedly applied these principles of statutory construction to require that materials blocked as “otherwise objectionable” have some relation to the universe of materials defined by the preceding statutory terms, *i.e.*, the blocked content must be akin to “obscene, lewd, lascivious, filthy, excessively violent, [or] harassing” materials. *See Song fi*, 108 F. Supp. 3d at 883 (“[W]hen a statute provides a list of examples followed by a catchall term (or ‘residual clause’) like ‘otherwise objectionable,’ the preceding list provides a clue as to what the drafters intended the catchall provision to mean. … Given the list preceding ‘otherwise objectionable,’—“obscene, lewd, lascivious, filthy, excessively violent, [and] harassing ...’—it is hard to imagine that the phrase includes, as YouTube urges, the allegedly artificially inflated view count associated with ‘Luv ya.’” (internal citations omitted)); *Nat’l Numismatic Certification, LLC v. eBay, Inc.*, 08-42, 2008 WL 2704404, at *25 (M.D. Fla. July

8, 2008) (rejecting argument "that Congress intended the general term 'objectionable' to [immunize restricting access to] an auction of potentially-counterfeit coins" because "the word ['objectionable'] is preceded by seven other words that describe pornography, graphic violence, obscenity, and harassment"); *Goddard v. Google, Inc.*, 08-2738, 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008) (adopting the reasoning of *Nat'l Numismatic Certification* on this point). Conversely, if "otherwise objectionable" has no objective content and can mean whatever a provider of interactive computer services claims it should mean, the categories of material that Congress has specifically identified and that precede "otherwise objectionable" are rendering superfluous. Malwarebytes' implausible reading of Section 230 should be rejected. "Congress could have written the statute more broadly, but it did not." *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016).

Malwarebytes has not contended—and cannot plausibly contend—that ESG programs are "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing." Moreover, ESG pled facts showing that its customers want to obtain, ***choose*** to download, and elect to ***pay*** for ESG software. *See* E.R. 26 at ¶ 17; E.R. 33 at ¶¶ 48-50. Plainly, those consumers do not find ESG programs "objectionable." Thus, because ESG programs are not remotely related to the content categories enumerated in the CDA,[3] Malwarebytes is not entitled to immunity under either sub-section of Section 230(c)(2).[4] *See Song fi*, 108 F. Supp. 3d at 883 ("[E]ven if the Court can 'see why artificially inflated view counts would be a problem for ... YouTube and its users,' … the terms preceding 'otherwise objectionable' suggest Congress did not intend to immunize YouTube from liability for removing materials from its website simply because those materials pose a 'problem' for YouTube." (internal citations omitted)); *Goddard*, 2008 WL 5245490, at *6 ("[T]he relevant portions of Google's Content Policy require that MSSPs provide pricing and cancellation information regarding their services.

[3] Malwarebytes argued to the district court that ESG products are "objectionable" because its own PUP criteria include "excessive or deceptive distribution, affiliate or opt-out bundling practices" and "aggressive or deceptive behavior especially surrounding purchasing or licensing"; Malwarebytes contended that it considers ESG products "potentially unwanted" and therefore "objectionable" on grounds "similar to the adware at issue in *Zango* and 'harassing' spam emails at issue in *Holomaxx*." E.R. 16. Yet Malwarebytes never explained—because no plausible explanation exists—how the amorphous distribution, purchasing or licensing practices referenced in its PUP policy are akin to the obscene, lewd, harassing or violent materials referenced in Section 230(c)(2)(A). Finally, ESG expressly pled that Malwarebytes does not actually consider ESG's programs to be harassing, otherwise objectionable, or a threat. *See* E.R. 53 at ¶¶ 124-25. Malwarebytes' claims to the contrary are inappropriate on a motion to dismiss.

[4] Section 230(c)(2)(A) provides the definition of material subject to the provision, *e.g.* "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Section 230(c)(2)(B), in turn, provides immunity for "any action taken to enable or make available … the technical means to restrict access to the materials described" in sub-section (A). *See supra* at n.1. Thus, immunity under sub-section (B) extends only to technical means that block those same materials.

These requirements relate to business norms of fair play and transparency and are beyond the scope of § 230(c)(2).”).

2. Malwarebytes’ Conduct Falls Outside the Express Terms of Section 230(c)(2)(B).

Sub-section (B) of Section 230(c)(2) immunizes actions that “enable or make available” to “others” the “technical means to restrict access” to materials described in sub-section (A). *See supra* at n.3. Malwarebytes’ conduct here falls outside this grant of immunity in two respects.

First, as previously demonstrated, ESG products are not “material” described in sub-section (A) as properly construed. ESG products are not obscene, lewd, lascivious, filthy, excessively violent, or harassing, nor can they be considered “otherwise objectionable” under any reasonable reading of sub-section (A).

Second, characterizing Malwarebytes’ conduct in unilaterally blocking and disabling ESG products—even when they have been purchased and paid for by ESG customers—as merely an “action” taken to “enable or make available” to “others” the “technical means” to restrict access to offensive materials would distort the CDA’s language beyond recognition. Indeed, Malwarebytes is not simply providing “technical means” that would enable users to restrict access to offensive materials. Rather, Malwarebytes blocks the download, installation and use of ESG programs on the ground that they are “potentially unwanted,” even when users affirmatively indicate they want those programs. E.R. 24-26 at ¶¶ 9, 16; E.R. 39-42 at ¶¶ 81-84; E.R. 44 at ¶ 92. Malwarebytes also provides no workable opt-out of its block, trapping users in a frustrating cycle of failed attempts to relaunch ESG programs with only a labyrinthine workaround , and has failed to provide adequate assistance to users who seek Malwarebytes' help to opt out of the block. *See* E.R. 24-26 at ¶¶ 10, 11, 17; E.R. 42-43 at ¶¶ 85-89; E.R. 44-45 at ¶¶ 90-95; E.R. 47-51 at ¶¶ 102-03, 108, 113-15. In doing so, Malwarebytes substitutes its own judgment for the consumer choice and user control Section 230 is intended to effectuate. Because it imposes its own position regarding a direct competitor's programs on users who have indicated they want those programs by downloading and purchasing them, Malwarebytes cannot shelter behind a claim that it merely provides "technical means" of blocking whose implementation others control.

In short, immunizing Malwarebytes' conduct under sub-section (B) would stand the plain purpose of that provision on its head.

3. Malwarebytes' Conduct Cannot be Deemed a Good Faith Exercise of the Activities Section 230(c)(2)(B) is Intended to Immunize.

The district court further erred by holding that sub-section (B) of Section 230(c)(2) does not require a provider of interactive computer services to act in good faith when it seeks immunity for its conduct. E.R. 6-7. Such a statutory interpretation fails to interpret the CDA as a whole and needlessly sacrifices internal consistency. *See Christensen v. C.I.R.*, 523 F.3d 957, 960 (9th Cir. 2008) ("[W]e do more than view words or sub-sections in isolation. We derive meaning from context, and this requires reading the relevant statutory provisions as a whole. … In addition, we look to the language of the statutory scheme as a whole to interpret the particular statutory provision." (internal quotations and citation omitted)).

Good faith is an implied requirement for any attempt to invoke the immunity extended under sub-section (B) when the "Good Samaritan" provision of the CDA is read as a whole.[5] *See generally Perez-Guzman v. Lynch*, 835 F.3d 1066, 1074 (9th Cir. 2016), *cert. denied sub nom. Perez-Guzman v. Sessions*, 138 S. Ct. 737 (2018) ("Our goal is to understand the statute as a symmetrical and coherent regulatory scheme and to fit, if possible, all parts into a harmonious whole." (internal quotations omitted)). While it is true that only sub-section (A) of Section 230(c)(2) explicitly requires that an "action" "to restrict access" be taken in "good

[5] Notably, when Malwarebytes first moved to dismiss the FAC, it correctly recognized that good faith was a requirement across both sub-sections of § 230(c)(2). *See* E.R. 21 ("A plaintiff asserting a claim against a provider of filtering software bears the burden of proving that a provider failed to act in good faith."). When given a second bite at the apple, however, Malwarebytes newly contended that § 230(c)(2)(B) does not require good faith, despite relying primarily on the same cases in their second Motion as they cited in their first. E.R. 15-16. Malwarebytes' initial acceptance of a good faith requirement before its about-face demonstrates that such a requirement makes sense and is consistent with the purpose of Section 230.

faith," the structure of Section 230(c)(2) necessarily applies the "good faith" requirement more broadly. The ***entire*** CDA Section 230(c), including Section 230(c)(2)(B), is captioned "Protection for '***Good Samaritan***' blocking and screening of offensive material" (emphasis added). It beggars belief that Congress intended to recognize an entity acting in bad faith as a "Good Samaritan," let alone to confer immunity on bad faith conduct. *See Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1163-64 (9th Cir. 2008) ("[T]he substance of section 230(c) can and should be interpreted consistent with its caption."). Indeed, it would be logically impossible for Congress to have intended to immunize an entity applying "technical means" in bad faith to disable and make unavailable ESG programs. So, too, it would be logically impossible for a party to act in good faith if it had in *bad faith* deemed the material to be restricted to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." In each case, it would be anomalous in the extreme—and a perversion of the CDA's purposes—if such bad faith conduct was to be immunized. Thus, contrary to the district court's holding, Section 230(c)(2)(B) requires that Malwarebytes act in good faith.

4. ESG Sufficiently Pleads that Malwarebytes Has Not Acted in "Good Faith."

Because the district court decided good faith action was not required to obtain immunity under Section 230(c)(2)(B), it did not address the adequacy of ESG's allegations of Malwarebytes' bad faith. This Court, however, should find that ESG has adequately pled that Malwarebytes has ***not*** acted in "good faith" and cannot therefore claim immunity under Section 230(c)(2). The FAC alleges that just one week before it was required to respond to the Subpoena in the Related Case—facing the prospect of having to produce documents and testify under oath regarding its involvement in Bleeping's anti-competitive conduct, which included funding a portion of Bleeping's defense costs in the Related Case—Malwarebytes revised its PUP criteria to "interfer[e] with ESG's current and prospective customer base, injur[e] ESG's business, and retaliat[e] against ESG[.]" E.R. 24 at ¶¶ 7-8; E.R. 27-28 at ¶ 25; E.R. 36-38 at ¶¶ 62, 64, 72-73. ESG also alleged that Malwarebytes' own CEO boasted about the PUP criteria revision on Malwarebytes' website, and Malwarebytes employees made clear in public statements that the revision was intended to target ESG. E.R. 24 at ¶ 7; E.R. 28-30 at ¶ 28-33; E.R. 39 at ¶ 78. ESG further alleges that MBAM had never before characterized ESG programs as PUPs and the revised criteria were created to target ESG's programs and track defenses asserted by Bleeping in the Related Case to assist in Bleeping's defense. E.R. 24 at ¶ 6; E.R. 27-28 at ¶¶ 25-27; E.R. 38 at

¶ 75. Finally, the FAC alleges that "Malwarebytes has no objective, good faith basis to claim that ESG's products" are "potentially unwanted" and that the consumer complaints quoted in the FAC establish that ESG "customers who have already downloaded (and paid for), or are trying to download, SpyHunter or RegHunter ***want*** those programs on their computer, a fact Malwarebytes knows." E.R. 54 at ¶ 126 (original emphasis).

In short, the FAC sets forth clear allegations that go far beyond the specificity required under the applicable notice-pleading standards[6] and support a plausible inference that Malwarebytes' blocking of ESG programs as PUPs was not undertaken in good faith. Malwarebytes and other cyber security software providers are free to develop and distribute, in good faith, filtering technologies

[6] Given the specificity of ESG's allegations, Malwarebytes' citations in its district court briefing to *Holomaxx Tech. v. Microsoft Corp.*, 783 F. Supp. 2d 1097 (N.D. Cal. 2011), and *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008), as alleged support for its argument are misplaced. In *Holomaxx*, plaintiff did not plead—as ESG pleads here—that defendant designed its "filtering technologies" specifically to target plaintiff in retaliation or to cause it harm. *Id*. at 1105. Rather, plaintiff pled "conclusorily that [defendant] acted in bad faith," alleging only that defendant was "'[p]ossibly seeking to cut costs in its free email service' and … on information and belief … profit[ed] from requiring senders to join 'whitelists[.]'" *Id*. In *e360Insight*, plaintiff did not plead *any* facts giving rise to a plausible inference of the absence of defendant's good faith. 546 F. Supp. 2d at 609. For this reason, the Court rejected plaintiff's argument that defendant acted in bad faith when it "allow[ed] numerous other companies to send bulk emails in greater volume and with greater frequency … singling out Plaintiff when other behaving in a like manner are not treated in a like fashion." *Id*. (also noting that Comcast did not claim that it refused to transmit e360's emails because of "their volume and their frequency").

that target materials that are in fact akin to "obscene, lewd, lascivious, filthy, excessively violent, [and] harassing" content. They may not, however, target competitors with demonstrably false allegations and prohibit their competitors' customers from using the software they want.

Indeed, in *Zango*, Judge Fisher expressed similar concerns as to the proper limits of the CDA. He explained that the CDA was not intended to and should not extend immunity to a party that "abuse[s] the immunity" by unilaterally "block[ing] content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material 'otherwise objectionable.'" 568 F.3d at 1178 (Fisher, J., concurring). He further explained that Section 230 should not protect a party who abuses the CDA by being "less accommodating to the user's preferences" either by "not providing an override option or making it difficult to use." *Id*.

Judge Fisher's concerns apply in full force to Malwarebytes' blocking of ESG's software. The FAC alleges facts showing that Malwarebytes revised its PUP criteria as a pretense to begin blocking its users' access to ESG programs at its malicious whim for anti-competitive purposes. E.R. 24 at ¶¶ 7-8; E.R. 27-28 at ¶¶ 21, 25-27; E.R. 36-38 at ¶¶ 67, 72-73, 76; E.R. 54 at ¶ 127. Additionally, Malwarebytes does ***not*** "enable" or effectuate user preference. To the contrary, many such users want to access ESG products, have complained to Malwarebytes about its unjustified blocking of their access, and cannot override Malwarebytes' designation of ESG products as PUPs and its quarantining and blocking of those products. *E.g.*, E.R. 25 at ¶ 11; E.R. 43-45 at ¶¶ 88-95; E.R. 48-53 at ¶¶ 103, 105-06, 109-11, 113-22.

Extending immunity to Malwarebytes for its unilateral, bad faith, anti-competitive blocking of ESG programs would abuse the grant of immunity Congress created "to facilitate users' access to blocking software that makes Internet use 'safer' than it otherwise would be." *Zango*, 568 F.3d at 1179 (Fisher, J., concurring).

* * *

Ultimately, Malwarebytes proposed, and the district court adopted, a construction of CDA Section 230(c)(2) that would allow any anti-malware software provider to block any other provider's competing products if the blocking provider deemed the blocked product "potentially unwanted" and therefore "otherwise objectionable." It would immunize that conduct regardless of whether the blocking provider had acted for anticompetitive reasons, on a "malicious whim," or in bad faith. This holding in effect allows ***anyone*** to block ***any content*** on the Internet ***for any reason*** as long as the blocking entity was willing to claim the blocked product was "objectionable" pursuant to its own undefined, arbitrary, and entirely personal standards. The district court's reading of Section 230 conflicts with the Congressional policies stated in the CDA, conflicts with the language and purposes of Section 230, and warrants reversal.

E. ESG's Lanham Act Claim is Not Subject to the CDA.

Even if § 230(c)(2) immunity were available to Malwarebytes for its blatantly anti-competitive behavior, which it is not, that immunity would ***not*** bar ESG's Lanham Act claim, contrary to the district court's holding. Section 230(e)(2) provides that "nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). "[O]n the basis of th[is] statutory text, … the CDA does not bar [a § 43(a)] Lanham Act claim." *Enigma Software Grp. USA v. Bleeping Computer LLC*, 194 F. Supp. 3d 263, 273-74 (S.D.N.Y. 2016); *see also Gen. Steel Dom. Sales, LLC v. Chumley*, 14-CV-01932-REB-CBS, 2015 WL 4911585, at *9 (D. Colo. Aug. 18, 2015), *appeal dismissed sub nom. Gen. Steel Dom. Sales, L.L.C. v. Chumley*, 840 F.3d 1178 (10th Cir. 2016) ("The § 1125 [false advertising] claim of the plaintiff is an intellectual property claim. Therefore, this claim does not fall within the ambit of § 230 immunity claimed by the defendants."); *Nieman v. Versuslaw, Inc.*, 12-3104, 2012 WL 3201931, at *8 (C.D. Ill. Aug. 3, 2012), *aff'd*, 512 Fed. Appx. 635 (7th Cir. 2013) ("[T]he Lanham Act claim would most certainly be considered an intellectual property claim."); *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (holding that CDA immunity did not extend to, *inter* *alia*, claims for "false designations of origin and false descriptions and representations under Section 43(a) of the Lanham Act").

The district court held to the contrary solely on the basis of *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1109-10 (C.D. Cal. 2004). That case, however, determined only that claims of false advertising under the California ***Business & Professions Code*** and ***common law*** did not pertain to "intellectual property" and were not subject to the CDA's intellectual property law exception. Unlike the precedent cited by ESG, *Perfect 10* did not address the Lanham Act, and so is inapposite.

IX. CONCLUSION

For the foregoing reasons, this Court should reverse the district court's dismissal of ESG's First Amended Complaint and judgment for Malwarebytes and remand for further proceedings.

X. STATEMENT OF RELATED CASES

ESG is not aware of any related cases pending in this Court.

Dated: April 2, 2018

Respectfully submitted,

By: /s/ Terry Budd

Terry Budd
BUDD LAW PLLC
120 Lyndhurst Circle
Wexford, PA 15090
Telephone: 412.613.2541
terry.budd@buddlawglobal.com

&

Christopher M. Verdini
Anna Shabalov
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
Telephone: 412.355.6500
Facsimile: 412.355.6501
christopher.verdini@klgates.com
anna.shabalov@klgates.com

&

Edward P. Sangster
K&L GATES LLP
Four Embarcadero Center, Suite 1200
San Francisco, CA 94111
Telephone: 415 882 8200
Facsimile: 415 882 8220
edward.sangster@klgates.com

Counsel for Plaintiff-Appellant

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 28.1(e)(3), I certify that this brief contains 11,383 words, which meets the type-volume limitation stated in Circuit Rule 28.1-1(c). This brief uses a proportional typeface and 14-point font.

Dated: April 2, 2018

/s/ Terry Budd
Terry Budd
BUDD LAW PLLC
120 Lyndhurst Circle
Wexford, PA 15090
Telephone: 412.613.2541
terry.budd@buddlawglobal.com

9th Circuit Case Number(s) 17-17351

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) 4/2/2018 .

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.

Signature (use "s/" format) s/Terry Budd

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)