



Neutral

As of: January 17, 2020 3:26 PM Z

## **Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.**

United States Court of Appeals for the Ninth Circuit

February 15, 2019, Argued and Submitted, San Francisco, California; December 31, 2019, Amended

No. 17-17351

### **Reporter**

2019 U.S. App. LEXIS 38784 \*; \_\_\_ F.3d \_\_\_; 2019 WL 7373959

ENIGMA SOFTWARE GROUP USA, LLC, Plaintiff-Appellant, v. MALWAREBYTES, INC., Defendant-Appellee.

**Prior History:** [\*1] Appeal from the United States District Court for the Northern District of California. D.C. No. 5:17-cv-02915-EJD. Edward J. Davila, District Judge, Presiding.

**Disposition:** REVERSED and REMANDED.

barred by [§ 230](#) of the Communications Decency Act of 1996, plaintiff computer security software provider's claims alleging that defendant, a direct competitor, configured its software to block users from accessing plaintiff's software in order to divert plaintiff's customers because as to plaintiff's state law claims, the phrase "otherwise objectionable" in the "Good Samaritan" provision of the Act, [§ 230\(c\)\(2\)](#), did not include software that the provider found objectionable for anticompetitive reasons, and plaintiff's allegations of anticompetitive animus were sufficient to withstand dismissal, and as to plaintiff's Lanham Act false advertising claim, [§ 230\(e\)\(2\)](#)'s exception for intellectual property claims did not apply because the false advertising claim did not relate to trademarks or any other type of intellectual property.

### **Core Terms**

---

immunity, provider, objectionable, block, software, users, intellectual property, district court, online, anticompetitive, programs, false advertising, internet, filtering, Lanham Act, trademarks, competitors, reasons, pornography, alleges, federal claim, harassing, offensive, violent, majority opinion, pertaining, encompass, unwanted, parties, computer service

### **Outcome**

Judgment reversed. Case remanded.

### **LexisNexis® Headnotes**

---

### **Case Summary**

---

#### **Overview**

HOLDINGS: [1]-The district court erred in dismissing, as

Communications Law > Federal Acts > Telecommunications Act > Communications Decency Act

[HNI](#) **Telecommunications Act, Communications Decency Act**

[47 U.S.C.S. § 230](#), the so-called Good Samaritan provision of the Communications Decency Act of 1996, was 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. [§ 230\(c\)\(2\)](#). The provision establishes a subjective standard whereby internet users and software providers decide what online material is objectionable.

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN2](#) **Telecommunications Act, Communications Decency Act**

The Communications Decency Act of 1996's immunity provision contains an exception for intellectual property claims, stating that nothing in this section shall be construed to limit or expand any law pertaining to intellectual property. [47 U.S.C.S. § 230\(e\)\(2\)](#).

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN3](#) **Telecommunications Act, Communications Decency Act**

The Communications Decency Act of 1996, which was enacted as part of the Telecommunications Act of 1996, contains a Good Samaritan provision that, in [47 U.S.C.S. § 230\(c\)\(2\)\(B\)](#), immunizes internet-service providers from liability for giving internet users the technical means to restrict access to the types of material described in the [§ 230\(c\)\(2\)\(A\)](#). 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. [§ 230\(c\)\(2\)\(A\)](#).

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN4](#) **Telecommunications Act, Communications Decency Act**

[47 U.S.C.S. § 230\(c\)](#) is entitled "Protection for Good Samaritan blocking and screening of offensive material." [Section 230\(c\)\(2\)](#), "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 [§ 230\(c\)\(2\)\(A\)](#). [§ 230\(c\)\(2\)\(A\), \(B\)](#).

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN5](#) **Telecommunications Act, Communications Decency Act**

Providers do not have unfettered discretion to declare online content "objectionable" and blocking and filtering decisions that are driven by anticompetitive animus are not entitled to immunity under [47 U.S.C.S. § 230\(c\)\(2\)](#).

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN6](#) **Telecommunications Act, Communications Decency Act**

The intellectual property exception to the Communications Decency Act of 1996's immunity provision states that [47 U.S.C.S. § 230](#) immunity shall not be construed to limit or expand any law pertaining to intellectual property. [§ 230\(e\)\(2\)](#).

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN7](#) **Telecommunications Act, Communications**

**Decency Act**

The Communications Decency Act of 1996 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\(b\)\(2\)-\(3\)](#). It gives providers discretion to identify objectionable content in large part to protect competition, not suppress it. [§ 230\(b\)\(2\)-\(3\)](#).

Governments > Legislation > Interpretation

**[HN8](#) [↓] Legislation, Interpretation**

The principle of ejusdem 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.

Governments > Legislation > Interpretation

**[HN9](#) [↓] Legislation, Interpretation**

Where the list of objects that precedes an "or other" phrase is dissimilar, ejusdem generis does not apply.

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

**[HN10](#) [↓] Telecommunications Act, Communications Decency Act**

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 Communications Decency Act of 1996 and the immunity would not apply.

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

**[HN11](#) [↓] Telecommunications Act, Communications Decency Act**

[Section 230\(e\)\(2\)](#) of the Communications Decency Act

of 1996 contains an exception to immunity for intellectual property claims. [47 U.S.C.S. § 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.

Antitrust & Trade Law > Consumer  
Protection > Likelihood of Confusion > False  
Designation of Origin

Antitrust & Trade Law > Consumer  
Protection > False Advertising > Lanham Act

Antitrust & Trade Law > Consumer  
Protection > Likelihood of Confusion > Trademark  
Infringement

**[HN12](#) [↓] Likelihood of Confusion, False Designation of Origin**

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. [15 U.S.C.S. § 1114](#). The latter, [15 U.S.C.S. § 1125](#), creates two bases of liability, false association and false advertising. [§ 1125\(a\)\(1\)\(B\)](#). 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.

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

**[HN13](#) [↓] Telecommunications Act, Communications Decency Act**

Because Congress did not define the term "intellectual property law" in the intellectual property exception contained in the Communications Decency Act of 1996's (CDA) immunity provision, it should be construed narrowly to advance the CDA's express policy of providing broad immunity. One of these express policy reasons for providing immunity was, as Congress stated in [47 U.S.C.S. § 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. [§ 230\(b\)\(2\)](#). The intellectual property exception is a limitation on immunity, and the CDA's 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.

Communications Law > Federal  
Acts > Telecommunications Act > Communications  
Decency Act

### [HN14](#) **Telecommunications Act, Communications Decency Act**

The intellectual property exception contained in [47 U.S.C.S. § 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 [15 U.S.C.S. § 1125\(a\)](#) of the Lanham Act, unless the claim itself involves intellectual property.

#### Summary:

SUMMARY\*\*

#### Communications Decency Act

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

Enigma Software Group USA, LLC, and Malwarebytes,

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

[Section 230](#), the so-called "Good Samaritan" provision of the Communications Decency Act, immunizes software providers from liability for actions taken to help users block certain types of unwanted online material, including material that is of a violent or sexual nature or is "otherwise **[\*2]** 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 relate to trademarks or any other type of intellectual property. The panel remanded the case for further proceedings.

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

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

Tyler G. Newby (argued), Guinevere L. Jobson, and Sapna Mehta, Fenwick & West LLP, San Francisco, California; Benjamin A. Field, Neal Kumar Katyal, and Reedy Swanson, Hogan Lovells US LLP, Washington, D.C.; for Defendant-Appellee. **[\*3]**

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

Venkat Balasubramani, Focal PLLC, Seattle, Washington; Eric Goldman, Professor; Jess Miers, Law

---

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

Student; Santa Clara University School of Law, Santa Clara, California; for Amici Curiae Cybersecurity Law Professors.

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

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

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

**Opinion by:** Mary M. Schroeder

## Opinion

---

AMENDED OPINION

SCHROEDER, Circuit Judge:

### OVERVIEW

[HN1](#)<sup>[↑]</sup> 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 [\[\\*4\]](#) 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 [\[\\*5\]](#) 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. [HN2](#)<sup>[↑]</sup> 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 [\[\\*6\]](#) 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

---

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

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\(c\)\(1996\)](#). [HN3](#)<sup>1</sup> 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 [\[\\*7\]](#) giving internet users the technical means to restrict access to the types of material described in the [subparagraph A](#). *Id.* [§ 230\(c\)\(2\)\(B\)](#). The material, as described in that subparagraph, is "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." *Id.* [§ 230\(c\)\(2\)\(A\)](#).<sup>1</sup>

This grant of immunity dates back to the early days of the internet when concerns first arose about children being able to access online pornography. Parents could

---

<sup>1</sup> [HN4](#)<sup>1</sup> [Section 230\(c\)](#) is entitled "Protection for 'Good Samaritan' blocking and screening of offensive material." The relevant [subsection \(2\)](#), "Civil liability," states, in full, as follows:

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

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

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

[47 U.S.C. § 230\(c\)\(2\)\(A\), \(B\)](#).

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 [\[\\*8\]](#) 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 N.Y. Misc. LEXIS 229, 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., 17 N.Y.3d 281, 952 N.E.2d 1011, 929 N.Y.S.2d 19 (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 [\[\\*9\]](#) 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 [\*10] 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, 117 S. Ct. 2329, 138 L. Ed. 2d 874 \(1997\)](#). 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 [\*11] restrict their children's access to objectionable or inappropriate online content"; and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services." See *id.* [§ 230\(b\)\(2\)-\(4\)](#).

This court has decided one prior case where we considered the scope of [§ 230](#), but were principally concerned with which types of online-service providers Congress intended to immunize. See [Zango, 568 F.3d at 1175](#). We acknowledged that providers of computer security software can benefit from [§ 230](#) immunity, and that such providers have discretion to identify what online content is considered "objectionable," *id.*, but we had no reason to discuss the scope of that discretion. The separate concurrence in *Zango* focused on the future need for considering appropriate limitations on provider control. See [id. at 1178-80](#) (Fisher, J.

concurring). District courts have differed in their interpretations of *Zango* and the discretion granted to providers. What is clear to us from the statutory language, history, and case law is that [HN5](#) providers do not have unfettered discretion to declare online content "objectionable" and blocking and filtering decisions that are driven by anticompetitive animus are not entitled to immunity [\*12] under [section 230\(c\)\(2\)](#).

## FACTUAL BACKGROUND

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

Providers of computer security software help users identify and block malicious or threatening software, termed malware, from their computers. Each provider generates its own criteria to determine what software might threaten users. Defendant Malwarebytes programs its software to search for what it calls Potentially Unwanted Programs ("PUPs"). PUPs include, for example, what Malwarebytes describes as software that contains "obtrusive, misleading, or deceptive advertisements, branding or search practices." Once Malwarebytes's security software is purchased and installed on a user's computer, it scans for PUPs, and according to Enigma's complaint, if the user tries to download a program that Malwarebytes has determined to be a PUP, a pop-up alert warns the user of a security risk and advises the user to stop the download and block the potentially threatening content. [\*13]

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 [\*14] 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 [\*15] 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 [HN6](#) 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 [\*16] 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 [\*17] 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 [\*18] 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 [\*19] 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 U.S. Dist. LEXIS 169939, 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 [\*20] 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 [\*21] 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. [HN7](#)<sup>[↑]</sup> 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, [\*22] 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 [\*23] 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 [HN8](#)<sup>[↑]</sup> the principle of *eiusdem generis*, which teaches that when a generic term follows specific terms, the generic term should [\*24] 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, 111 S. Ct. 1156, 113 L. Ed. 2d 95 \(1991\)](#). 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 \(9th Cir. 1990\)](#)[HN9](#)<sup>[↑]</sup> ("Where the list of objects that precedes the 'or other' phrase is dissimilar, *eiusdem 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 *eiusdem 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 *eiusdem generis*. Several district courts have, for example, regarded [\*25] 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 U.S. Dist. LEXIS](#)

[43360, 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. [HN10](#) [↑] 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. [\*26]

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.

[HN11](#) [↑] [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 [\*27] 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.

[HN12](#) [↑] 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, [\*28] . . . [§ 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, 123 S. Ct. 2041, 156 L. Ed. 2d 18 \(2003\)](#).

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").

[HN13](#) [↑] 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 [\*29] 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.*

[HN14](#)<sup>[↑]</sup> 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 [\*30] 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.**

**Dissent by:** Johnnie B. Rawlinson

## Dissent

---

RAWLINSON, Circuit Judge, dissenting:

In his concurring [\*31] opinion in [Zango, Inc. v. Kaspersky Lab, Inc.](#), 568 F.3d 1169, 1179-80 (9th Cir. 2009), Judge Fisher acknowledged that "until Congress clarifies the statute or a future litigant makes the case for a possible limitation," the "broadly worded" Communications Decency Act (the Act) afforded immunity to a distributor of Internet security software. Congress has not further clarified the statute and Enigma Software has not persuasively made a case for limitation of the statute beyond its provisions.

The majority opinion seeks to limit the statute based on the fact that the parties are competitors. *See Majority Opinion*, p. 6. However, nothing in the statutory provisions or our majority opinion in *Zango* supports such a distinction. Rather the "broad language" of the Act specifically encompasses "any action voluntarily taken [by a provider] to restrict access to . . . material that the provider . . . considers to be . . . otherwise objectionable." [47 U.S.C. § 230\(c\)\(2\)\(A\)](#) (emphasis added). Under the language of the Act, so long as the provider's action is taken to remove "otherwise objectionable" material, the restriction of access is immunized. *See id.* The majority's real complaint is not that the district court construed the statute too broadly, but that the statute is written too broadly. [\*32] 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, 192 L. Ed. 2d 208 (2015).

In particular, the majority holds that the criteria for blocking online material may not be based on the identity of the entity that produced it. *See Majority Opinion*, p. 11. Unfortunately, however, that conclusion cannot be squared with the broad language of the Act.

Under the language of the statute, if the blocked content is "otherwise objectionable" to the provider, the Act bestows immunity. [Zango, 568 F.3d at 1173](#) ("[T]he statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user *or the provider* deems objectionable.") (emphasis in the original); [1174](#) ("Accordinging 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 [\[\\*33\]](#) 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, 112 S. Ct. 1146, 117 L. Ed. 2d 391 \(1992\)](#) (citations omitted).

I respectfully dissent.