CHAPMAN LAW REVIEW

CHAPMAN UNIVERSITY | FOWLER SCHOOL OF LAW | ONE UNIVERSITY DRIVE | ORANGE, CALIFORNIA 92866
WWW.CHAPMANLAWREVIEW.COM

A Crack in the Armor: The Ninth Circuit's Improper Limitation on the Scope of Section 230 Immunity in *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*

Madeleine Dobson[*]

[*] J.D. Candidate, expected May 2022, Chapman University Dale E. Fowler School of Law. B.A. University of California, Berkeley, 2017. Thank you to Dean Marisa S. Cianciarulo for her guidance and invaluable feedback during the writing process. Thank you also to Professor Sherry Leysen for her advice and research support. Many thanks to the entire *Chapman Law Review* editorial staff for their thoughtful revisions. Lastly, thanks to my family and friends for all of their encouragement and support during law school.

INTRODUCTION

Section 230 of the Communications Decency Act has been called the twenty-six words that created the internet.[1] In short, Section 230 provides a safe harbor to website providers for moderating[2] objectionable content on their sites, allowing them to avoid civil liability for much of what occurs online.[3] It has been invoked by a wide-range of website providers like Twitter,[4] Facebook,[5] Tumblr,[6] Myspace,[7] YouTube,[8] Airbnb,[9] eBay,[10] Yelp,[11] and Craigslist[12] to immunize against claims brought by internet users, including

[1] *See* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 1–2 (2019).

[2] Moderation refers to both a website provider's decision to *remove* content from their site, and well as its decision to leave the content up on its website, as claims such as defamation can be brought against it by allowing the information to remain online. *See* VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 46 (2002) (explaining that Section 230 immunizes providers' decisions "both to host and *not* to host user content . . .").

[3] *See* 47 U.S.C. § 230(c).

[4] *See generally* Murphy v. Twitter, Inc., 274 Cal. Rptr. 3d 360, 363, 369 (Cal. Ct. App. 2021) (invoking Section 230 successfully against claims for breach of contract, promissory estoppel, and violation of California unfair competition law).

[5] *See generally* Force v. Facebook, Inc., 934 F.3d 53, 57 (2d Cir. 2019) (relying on Section 230 to avoid civil liability for federal anti-terrorism claims).

[6] *See generally* Poole v. Tumblr, Inc., 404 F. Supp. 3d 637, 639 (D. Conn. 2019) (utilizing Section 230 immunity to dismiss common law claims of invasion of privacy and negligent infliction of emotional distress).

[7] *See generally* Riggs v. MySpace, Inc., 444 F. App'x 986, 987 (9th Cir. 2011) (relying on Section 230 to defend claims of negligence and gross negligence arising from Myspace's decisions to delete user profiles).

[8] *See generally* Prager Univ. v. Google LLC, No. 19-340667, 2019 WL 8640569, at *12 (Cal. Super. Ct. Nov. 19, 2019) (claiming Section 230 based on YouTube's content restrictions).

[9] *See generally* La Park La Brea A LLC v. Airbnb, Inc., 285 F. Supp. 3d 1097, 1099–1100 (C.D. Cal. 2017) (invoking Section 230 against claims related to Airbnb rentals).

[10] *See generally* Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 706 (Cal. Ct. App. 2002) (using Section 230 to immunize against claims of unfair business practices, and a California memorabilia law).

[11] *See generally* Kimzey v. Yelp! Inc., 836 F.3d 1263, 1265–66 (9th Cir. 2016) (explaining that plaintiff's "creative" pleadings trying to circumvent Section 230 were futile and awarding immunity to Yelp).

[12] *See generally* Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 965, 968 (N.D. Ill. 2009) (extending immunity to Craigslist despite "adult services" advertisements being left on the site).

defamation,[13] breach of contract,[14] misappropriation of the right of publicity,[15] and even products liability.[16]

Historically, courts have construed Section 230 broadly in favor of a wide scope of immunity, reasoning that website providers may have an infinite number of users constantly generating large volumes of online content, making it difficult to moderate online material.[17]

But Section 230's expansive scope has frustrated presidents, members of Congress, and Supreme Court Justices, alike. Specifically, President Biden and former President Trump have each called for Section 230's repeal, indicating that both sides of the aisle share concerns about "Big Tech's"[18] inordinate power over the internet.[19] Further, there were twenty-six bills introduced during the last Congress involving Section 230, some of which sought to repeal it completely while others sought to narrow its scope.[20]

[13] *See, e.g.*, Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398 (6th Cir. 2014). In fact, the majority of Section 230 decisions involve defamation claims. Elizabeth Banker of the Internet Association estimated that forty-three percent of Section 230 decisions involve claims of defamation. The next largest category of claims was related to the First Amendment, representing roughly ten percent of Section 230 decisions. *See* Elizabeth Banker, *A Review of Section 230's Meaning & Application Based on More Than 500 Cases*, INTERNET ASS'N 2, http://internetassociation.org/wp-content/uploads/2020/07/IA_Review-Of-Section-230.pdf [http://perma.cc/86FS-WD2W] (last visited Mar. 20, 2022).

[14] *See, e.g.*, Murphy v. Twitter, Inc., 274 Cal. Rptr. 3d 360 (Cal. Ct. App. 2021). In this case, the breach of contract claim referred to the breach of the user agreement between the user and the operator, Twitter. *See id.*

[15] *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

[16] Bolger v. Amazon.com, LLC, 267 Cal. Rptr. 3d 601, 604 (Cal. Ct. App. 2020).

[17] *See* Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 18–19 (1st Cir. 2016); *see also* discussion *infra* Section I.D.

[18] "Big Tech" refers to the largest and most dominant technology companies, such as Google, Amazon, Facebook, Apple, and Microsoft. *See* Shannon Flynn, *What Is Big Tech and Why Is the Government Trying to Break It Up?*, MUO (Aug. 21, 2021), http://www.makeuseof.com/what-is-big-tech-and-why-is-the-government-trying-to-break-it-up-/ [http://perma.cc/YT52-5QR4].

[19] *See* Bryan Pietsch, *Trump and Biden Both Want to Revoke Section 230, But For Different Reasons*, BUS. INSIDER (May 30, 2020, 4:15 AM), http://www.businessinsider.com/trump-biden-want-to-revoke-section-230-for-different-reasons-2020-5 [http://perma.cc/ES5Q-UWJQ]; *see also* Shira Ovide, *What's Behind the Fight Over Section 230*, N.Y. TIMES (Mar. 25, 2021), http://www.nytimes.com/2021/03/25/technology/section-230-explainer.html [http://perma.cc/Y6YE-9DET] ("Republicans and Democrats are asking whether the law gives tech companies either too much power or too little responsibility for what happens under their watch."). During his campaign, President Biden expressed the need for internet reform, indicating that Section 230 should be revoked "immediately." The Editorial Board, *Joe Biden*, N.Y. TIMES (Jan. 17, 2020), http://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html?smid=nytcore-ios-share [http://perma.cc/F6HA-LEC9]. However, he has yet to make internet reform a legislative priority. *See* Eric Goldman, *Tech Policy in President Biden's First 100 Days*, 2021 U. ILL. L. REV. ONLINE 176, 176 (2021).

[20] VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 30 (2002).

Section 230 has also caught the attention of the United States Supreme Court, which has yet to consider a case under this provision.[21] But, as discussed below, at least one justice believes this is an area ripe for judicial intervention if Congress does not act.[22]

Since its enactment in 1996, there has been extensive exploration of this safe harbor by the legal and academic community, including Section 230's implications on the Fair Housing Act,[23] its interaction with the First Amendment,[24] and, most recently, its connection to "fake news" and the spread of disinformation.[25] Across subject areas, scholars have consistently questioned the broad scope of liability extended to website providers by Section 230, calling it "licensed anarchy,"[26] "immoral,"[27] and a "shield for scoundrels,"[28] and arguing that it has led to a "lawless internet"[29] by creating "monstrous"[30] platforms.[31]

In other words, it has become increasingly apparent that this statute, enacted two years before Google had even incorporated, is largely inadequate to address the perils of the modern-day

[21] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 13 (2020) ("[I]n the 24 years since [Section 230's enactment], we have never interpreted this provision. But many courts have construed the law broadly to confer sweeping immunity on some of the largest companies in the world.").

[22] *See* Doe v. Facebook, Inc., 142 S. Ct. 1087, 1088 (2022) ("Assuming Congress does not step in to clarify § 230's scope, we should do so in an appropriate case."); s*ee also* discussion *infra* Section III.C.

[23] *See, e.g.*, Jennifer C. Chang, *In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet*, 55 STAN. L. REV. 969 (2002).

[24] *See, e.g.*, Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019); *see also* Haley Griffin, *Laws in Conversation: What the First Amendment Can Teach Us About Section 230*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 473 (2021).

[25] *See, e.g.*, Erica O'Connell, *Navigating the Internet's Information Cesspool, Fake News and What to Do About It*, 53 U. PAC. L. REV. 251 (2022).

[26] Thomas D. Huycke, *Licensed Anarchy: Anything Goes on the Internet? Revisiting the Boundaries of Section 230 Protection*, 111 W. VA. L. REV. 581 (2009).

[27] Ali Grace Zieglowsky, *Immoral Immunity: Using a Totality of the Circumstances Approach to Narrow the Scope of Section 230 of the Communications Decency Act*, 61 HASTINGS L.J. 1307 (2009).

[28] David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 373 (2010).

[29] Colby Ferris, *Communication Indecency: Why the Communications Decency Act, and the Judicial Interpretation of It, Has Led to A Lawless Internet in the Area of Defamation*, 14 BARRY L. REV. 123 (2010).

[30] Natalie Annette Pagano, *The Indecency of the Communications Decency Act* § *230: Unjust Immunity for Monstrous Social Media Platforms*, 39 PACE L. REV. 511 (2018).

[31] *See* Nicole Phe, *Social Media Terror: Reevaluating Intermediary Liability Under the Communications Decency Act*, 51 SUFFOLK U. L. REV. 99, 116 (2018) (explaining that the overly broad construction of § 230 has led to an "overexpansion of immunity and resulted in near absolute invulnerability for [Internet Service Providers].").

internet.[32] As the Second Circuit has observed, "[o]ver the past two decades 'the Internet has outgrown its swaddling clothes,' and it is fair to ask whether the rules that governed its infancy should still oversee its adulthood."[33]

Instead of allowing Congress to properly reform this antiquated statute, a recent decision from the Ninth Circuit significantly limited the scope of immunity afforded under Section 230.[34] The case, *Enigma Software Group USA, LLC v. Malwarebytes, Inc.* ("*Enigma*"), is one of the rare decisions where a court denied immunity to an internet provider under Section 230.[35] By emphasizing non-textual arguments involving the policy and purpose of the statute, the Ninth Circuit ignored the plain language of the statute, imposed an implied good faith requirement, and in essence crafted a new exception from Section 230, initiating the "first chip in the immunity armor for makers of malware software."[36]

This Note examines the Ninth Circuit's unusual ruling and proceeds as follows. Part I provides a statutory overview to briefly explain the statute's history and legislative intent, the language of the provision, and Congress' express policy goals. Part I also addresses the foundational case of *Zango, Inc. v. Kaspersky Lab, Inc.*,[37] in which a prescient concurring opinion from the Ninth Circuit set the stage for the Ninth Circuit's policy considerations in the *Enigma* case. Part II discusses the Ninth Circuit's decision in *Enigma*, including the district court's initial grant of immunity and the Ninth Circuit's subsequent reversal. Part III describes the regressive results stemming from the Ninth Circuit's decision in *Enigma*, explaining that these implications defeat the very reason that the statute was enacted. Part III also identifies a split that has been created between the Ninth Circuit and a district court within the Fifth Circuit, as well as a clear split between the federal and state courts of California. Part IV examines the ways in which the Ninth Circuit violated the principles of statutory construction, arguing that the Ninth Circuit improperly disregarded the

[32] Andrew P. Bolson, *Flawed but Fixable: Section 230 of the Communications Decency Act at 20*, 42 RUTGERS COMPUT. & TECH. L.J. 1, 17 (2016).

[33] Force v. Facebook, Inc., 934 F.3d 53, 88 (2d Cir. 2019) (quoting Fair Housing v. Roomates.com, 521 F.3d 1157, 1175 n.39 (9th Cir. 2008)).

[34] *See* Gregory P. Szewczyk et al., *Weakened Privacy and Information Security Tools—the Unintended Consequence of Attacks on Section 230 of the CDA,* CYBERADVISER (Oct. 21, 2020), http://www.cyberadviserblog.com/2020/10/weakened-privacy-and-information-security-tools-the-unintended-consequence-of-attacks-on-section-230-of-the-cda/ [http://perma.cc/37BG-NK43].

[35] 938 F.3d 1026 (9th Cir. 2019).

[36] *See* Szewczyk et al., *supra* note 34.

[37] 568 F.3d 1169 (9th Cir. 2009).

statute's plain language in favor of policy considerations, added new statutory requirements despite Congress' clear omission, and created additional carve-outs from immunity. Part IV also looks to prior decisions that served as the impetus behind new statutory exceptions and sets forth how the Ninth Circuit should have properly proceeded. Finally, this Note concludes that *Enigma* decision defeats the very reason that the statute was enacted.

I. THE HISTORY, PLAIN LANGUAGE, AND PURPOSE OF SECTION 230

A. A Brief History of Section 230 of the Communications Decency Act

The Communications Decency Act was primarily enacted to protect children from sexually explicit online content and to make the internet a more family-friendly space.[38] But it was also enacted as a response to cases that held website providers liable as publishers[39] for defamatory comments posted by users on the site.[40] Specifically, it overruled *Stratton Oakmont, Inc. v. Prodigy Services Co.* ("*Stratton Oakmont*"), where a website provider was held liable for defamatory comments posted by anonymous users on its messaging boards.[41]

Lawmakers worried that the *Stratton Oakmont* decision would have a chilling effect on content moderation, recognizing that providers would likely refrain from moderating online content at all for fear that they would be treated as a publisher.[42] Indeed, "*Stratton Oakmont's* legal conclusion created a Hobson's choice for platforms' content moderation: either moderate content and face liability for all posts on your bulletin board, or don't moderate and have posts filled with obscenity."[43] Without any

[38] *See* Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003); *see also Force,* 934 F.3d at 63.

[39] By holding a website provider liable as a "publisher," it means that they receive the same treatment as the original content creator (i.e., the website user). *See* Ardia, *supra* note 28, at 397.

[40] *See, e.g.*, Yaffa A. Meeran, *As Justice So Requires: Making the Case for A Limited Reading of § 230 of the Communications Decency Act*, 86 GEO. WASH. L. REV. 257, 282 (2018);); *Batzel*, 333 F.3d at 1026.

[41] *See generally* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (holding that because the website provider was exercising some control over the bulletin boards, it should be treated as the publisher of the content and treated as the primary content creator); *cf.* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (refusing to hold a website provider liable for defamation based on a third-party user's comments on the site unless the website provider knew or had reason to know that the content was defamatory).

[42] *See* Bolson, *supra* note 32, at 5–6; *see also id.* at 7 (providing the statement by Representative Christopher Cox stating that website providers "are going to face higher . . . liability because [the providers] tried to exercise some control over offensive material").

[43] Adam Candeub, *Reading Section 230 as Written*, 1 J. FREE SPEECH L. 139, 142 (2021).

moderation, the internet would become a dangerous environment for users, especially children.[44]

Accordingly, Representatives Christopher Cox and Ron Wyden introduced the "Protection for Private Blocking and Screening of Offensive Material" bill, which was eventually codified as Section 230 in 1996.[45] Representative Cox explained that the legislation was intended to strike a balance between regulating indecent online material, while still allowing the Internet to develop without crippling regulation.[46] As one scholar has noted, the "twin goals" for Section 230 were to "foster[] open forums for online speech, while allowing users—and not courts—to dictate any restrictions on that speech."[47]

To achieve this balance, Section 230 incentivizes website providers to self-regulate indecent material on their sites by providing them with a safe harbor from civil liability based on that moderation, with certain enumerated exceptions.[48] As the First Circuit has explained, "Congress sought to encourage websites to make efforts to screen content without fear of liability."[49]

B. The Good Samaritan Provision

Section 230, which has been referred to as the "Good Samaritan" provision, contains two distinct provisions that shield internet providers from civil liability: section 230(c)(1) and section 230(c)(2).[50] Though section 230(c)(1) has been litigated and invoked much more frequently than section 230(c)(2), section 230(c)(2) is arguably the subject of much more scholarship and debate.[51] section 230(c)(2) also appears to be a greater source of

[44] *See* Bolson, *supra* note 32, at 6.

[45] *See id.* at 5.

[46] *See id.* at 8; *see also* Meeran, *supra* note 40, at 266.

[47] See KOSSEFF, *supra* note 1, at 207.

[48] Congress lists five statutory exceptions where providers are not shielded from liability by Section 230: (1) criminal law, (2) intellectual property law, (3) state law, (4) communications privacy law, and (5) sex trafficking law. 47 U.S.C. § 230(e).

[49] *See* Doe v. Backpage.com, LLC, 817 F.3d 12, 19 (1st Cir. 2016).

[50] 47 U.S.C. § 230.

[51] *See* Candeub, *supra* note 43, at 146 ("While section 230(c)(2) dominated the legislative discussion, section 230(c)(1) has dominated judicial decisions."); *see also* Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. IRVINE L. REV. 659, 660 (2012) [hereinafter *Online User Account Termination*]; *see also* Banker, *supra* note 13, at 3 ("Section 230 protects providers who engage in content moderation, but typically through application of subsection (c)(1) rather than the good faith provision, (c)(2)."); *see also* Ardia, *supra* note 28, at 412 n.194 (listing cases based on 47 U.S.C. § 230(c)(2)).

> The vast majority of Section 230 caselaw involves 230(c)(1), which has become the foundation of the modern Internet. In contrast, Section 230(c)(2) gets a lot less attention, for several reasons. First, content removal generally produces less litigation than continued content publication. Second, liability for content removal often can be handled through a variety of risk management techniques, including contract provisions. Third, Section 230(c)(2)(A) has a

confusion for courts, as some have collapsed the distinction between section 230(c)(2)(A) and section 230(c)(2)(B) entirely.[52]

In short, section 230(c)(1) and section 230(c)(2) confer broad protection to companies whether they decide to keep the "objectionable" information on their site or if they decide to remove it. The immunity contained in Section 230 appears in subsection (c) as follows:

> (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).[53]

First, section 230(c)(1) provides that "no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided," meaning that website providers are immune from liability and will not be treated as publishers[54] if they choose to keep user-created indecent material

> "good faith" requirement that is riskier and more expensive to litigate than Section 230(c)(1), which has no parallel scienter requirement . . . .
>
> Because of this, Section 230(c)(2) has largely receded in importance. However, Section 230(c)(2)(B) still provides foundational protection in one critical context: anti-threat software.

Eric Goldman, *Terrible Ninth Circuit 230(c)(2) Ruling Will Make the Internet More Dangerous–Enigma v. Malwarebytes*, TECH. & MKTG. L. BLOG (Sept. 19, 2019) [hereinafter *Terrible Ninth Circuit Ruling*], http://blog.ericgoldman.org/archives/2019/09/terrible-ninth-circuit-230c2-ruling-will-make-the-internet-more-dangerous-enigma-v-malwarebytes.htm [http://perma.cc/4RHY-H6PC].

[52] *See* BRANNON & HOLMES, *supra* note 2, at 8.

[53] 47 U.S.C. § 230 (emphasis added).

[54] 47 U.S.C. § 230(c)(1) addresses the publisher vs. distributor distinction that was at issue for website providers in the *Stratton Oakmont* decision. While a distributor enjoys the presumption of non-liability, a publisher is presumed to have knowledge of the content and is essentially treated the same as the primary content creator under the law. *See* Ardia, *supra* note 28, at 397–98.

on their websites, subject to several statutory exclusions.[55] A "classic example" of (c)(1) immunity is when:

> A Facebook user posts a defamatory statement, and the defamed plaintiff sues Facebook on the theory that, by allowing the post to stay up on its site, Facebook acted as a publisher of the post. The plaintiff's cause of action would include an element that treats the platform as "a publisher or speaker" of the user's words. Section 230(c)(1) would bar the action against Facebook, leaving the only action available to the plaintiff to be one against the user.[56]

Second, section 230(c)(2) protects website providers that choose to *restrict* access to objectionable information on their sites.[57] Within section 230(c)(2), there is a further distinction between subsections 230(c)(2)(A) and 230(c)(2)(B).[58]

Section 230(c)(2)(A) is implicated when a website provider *unilaterally* restricts access to material that the provider subjectively considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[59] For example, this paragraph is implicated when Facebook decides to remove something from the Facebook site that it deems to be objectionable.[60]

On the other hand, section 230(c)(2)(B) is implicated when the internet provider merely provides users with the "technical means" to restrict access to online material (i.e., a filtering tool), and the *user* rather than the *provider* elects to filter out

[55] *See* 47 U.S.C. § 203(c)(1). There has been some confusion regarding the scope of subsection (c)(1) and whether it applies to content that is kept up on a website as well as content that is removed from a website. As Valerie C. Brannon and Eric N. Holmes recently explained:

> One conception of these two provisions is that Section 230(c)(1) applies to claims for content that is "left up," while Section 230(c)(2) applies to claims for content that is "taken down." In practice, however, courts have also applied Section 230(c)(1) to "take down" claims, and courts sometimes collapse Section 230's two provisions into a single liability shield or do not distinguish between the two provisions.

BRANNON & HOLMES, *supra* note 2, at 8. However, reading subsection (c)(1) as immunizing both content that is left up and content that is taken down would render subsection (c)(2) superfluous. *See* Gregory M. Dickinson, *An Interpretive Framework for Narrower Immunity Under Section 230 of the Communications Decency Act*, 33 HARV. J.L. & PUB. POL'Y 863, 869–70 (2010); *see also* Candeub, *supra* note 43, at 151 (explaining that reading Section 230(c)(1) as protecting decisions to "take down" content essentially reads subsection (c)(2) out of the statute). A recent statement by Justice Thomas seems to clarify the meaning of (c)(1) as he wrote, "[i]n short … if a company unknowingly leaves up illegal third-party content, it is protected from publisher liability by §230(c)(1); and if it takes down certain third-party content in good faith, it is protected by §230(c)(2)(A)." *See* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 15 (2020).

[56] *See* Candeub, *supra* note 43, at 147.

[57] *See* 47 U.S.C. § 203(c)(2).

[58] *See id.*

[59] *See* 47 U.S.C. § 203(c)(2)(A).

[60] *See, e.g.*, Dipp-Paz v. Facebook, No. 18-CV-9037(LLS), 2019 WL 3205842 (S.D.N.Y. July 12, 2019).

objectionable material using the provider's technical means (e.g., YouTube gives users a filtering tool, and the user then elects to block out content by using the filtering tool).[61]

Notably, the language in section 230(c)(2)(A) plainly imposes a good faith limitation on the internet provider, requiring that any action taken by the website provider to remove objectionable content be taken "in good faith."[62] However, section 230(c)(2)(B) omits the good faith language, seemingly imposing no such requirement when website providers are merely providing users with a filtering tool to block content.[63]

In terms of policy, Congress' omission of a good faith requirement in section 230(c)(2)(B) makes good sense. Under section 230(c)(2)(A) immunity, providers are the sole decision-makers in whether to restrict user content from their website. Requiring them to act in good faith in their determination of what content qualifies as "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" ensures that content is not restricted for improper reasons.[64]

However, section 230(c)(2)(B) is implicated where the *users* are electing to filter certain content, and the website providers are merely providing the filtering technology. As explained by the Internet Association:[65]

> [S]ubsection (B) only applies where service providers put blocking tools in the hands of users, who must independently and affirmatively decide to use those tools . . . In this scenario, Congress logically concluded it was unnecessary to include a good faith requirement or to allow Section 230's protection to turn on disputes about a service provider's motives.

[61] *See, e.g.*, Ord. After Hearing, Prager Univ. v. Google LLC, No. 19CV340667, 2019 WL 8640569 (Cal. Super Nov. 19, 2019); *see also* Brief of Internet Association as Amicus Curiae In Support of Petitioner at 3, Enigma Software Group USA LLC v. Malwarebytes, Inc., 592 U.S. 1 (2020) (No. 19-1284) ("IA's members and many other online service providers regularly rely on this immunity in developing and deploying a range of user-empowering tools, including Twitter's 'block' and 'mute' features, YouTube's Restricted Mode, Reddit's user-moderated forums, and Microsoft's Office 365 Advanced Threat Protection.").

[62] *See* 47 U.S.C. § 230(c)(2)(A).

[63] *See* 47 U.S.C. § 230(c)(2)(B).

[64] *See* Nicholas Conlon, *Freedom to Filter Versus User Control: Limiting the Scope of § 230 (C)(2) Immunity*, 2014 U. ILL. J. L. TECH. & POL'Y 105, 113 (2014) (explaining that when the provider's filtering technology does not exhibit user control, under subsection (c)(2)(A), the statute requires that the provider act in good faith in its belief that its filtering accommodates user preferences).

[65] The Internet Association was a leading lobbying group for the technology industry, representing large, global internet companies such as Google, Facebook, Yahoo!, Amazon, and others. *See The Unified Voice of the Internet Economy*, INTERNET ASS'N, http://internetassociation.org/wp-content/uploads/2013/02/Fact-Sheet.pdf [http://perma.cc/CH4E-C3H2].

> Here, the user's independent choice operates as a check on the provider's decisions about what material should be filtered or blocked.[66]

Under this subsection, providers rightly bear less responsibility to ensure that filtered content is objectionable because the provider has ceded power to the user and maximized user control.[67] Thus, Congress' clear distinction between subsections (c)(2)(A) and (c)(2)(B) is a "trade-off between power and responsibility," meaning that when the provider relinquishes filtering power to users, it make little sense that they should face liability predicated on the user's filtering choices.[68]

Yet the Ninth Circuit seems to disagree, becoming the only decision on record to impose an implicit good faith requirement into section 230(c)(2)(B), for reasons that are explored in-depth below.[69]

C. The Statute's Express Policy Goals

In addition to the grant of immunity provided in section 230(c), Congress took the somewhat unusual step of stating policy goals directly in the statute. The five policy goals, which the Ninth Circuit relies on heavily to justify its disregard of the statutory text in *Enigma*, are as follows:

> (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.[70]

D. The Ninth Circuit's Approach to Immunity

Consistent with these policy goals, courts have traditionally interpreted the provisions of Section 230 broadly to confer wide

[66] Brief of Internet Association, *supra* note 61, at 21–22.
[67] *See* Conlon, *supra* note 64, at 113.
[68] *See id.*
[69] *See* discussion *infra* Section II.C.
[70] 47 U.S.C. § 230(b)(1)–(5).

immunity to website providers.[71] Indeed, as the First Circuit has noted, there has been "near-universal" agreement that Section 230 "should not be construed grudgingly," with the Ninth Circuit explaining that close cases should be resolved in favor of immunity.[72]

Like other courts, the Ninth Circuit has continued to interpret Section 230 expansively.[73] However, the Ninth Circuit's decision in *Zango, Inc. v. Kaspersky Lab, Inc.* ("*Zango*"),[74] arguably laid the foundation for the Ninth Circuit's significant limitation on the scope of liability nearly a decade later in *Enigma*.

In 2009, the Ninth Circuit considered whether providers of Internet security software were entitled to immunity under Section 230.[75] Zango, Inc. provided internet users with a free catalog of videos, games, music, tools, etc., while Kaspersky Lab, Inc. ("Kaspersky") provided internet users with security software that flagged certain internet programs as potentially malicious software, known as "malware."[76] After Kaspersky designated a program as malware, users would be warned of the harmful designation and were prompted with the option to allow or reject the download of the potentially harmful program.[77]

In this case, Kaspersky classified Zango Inc.'s programs as "potentially harmful" and internet users were warned that these

[71] *See* Gregory M. Dickinson, *An Interpretive Framework for Narrower Immunity Under Section 230 of the Communications Decency Act*, 33 HARV. J.L. & PUB. POL'Y 863, 867 (2010) ("Courts have, from the beginning, adopted a broad view of Section 230 immunity."); *see also* Ryan J.P. Dyer, *The Communication Decency Act Gone Wild: A Case for Renewing the Presumption Against Preemption*, 37 SEATTLE U. L. REV. 837, 842 (2014) ("[T]he first courts to interpret and apply section 230 went 'further than was necessary to effectuate the congressional goals' of the statute's immunity-granting provision. Although unapparent at first, this over-expansive reading of section 230(c) laid the groundwork for broad applications of immunity by future courts in contexts blatantly incommensurate with the statutes intended scope and effect."); *see also* Force v. Facebook, Inc., 934 F.3d 53, 64 (2d Cir. 2019) ("In light of Congress's objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity."); *see also* Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted [Section 230] to establish broad . . . 'immunity.'").

[72] *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008) ("[T]here will always be close cases . . . [s]uch close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230.").

[73] *See, e.g.*, *id.*; *see also* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1108 (9th Cir. 2007) (stating that the Communications Decency Act provides a "broad grant of immunity"); *see also* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (citing to Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003), which "joined the consensus developing across other courts of appeals that § 230(c) provides broad immunity").

[74] 568 F.3d 1169 (9th Cir. 2009).

[75] *Id.* at 1170.

[76] *Id.*

[77] *Id.* at 1171.

programs contained possible malware.[78] While Zango, Inc. asserted claims against Kaspersky, Kaspersky invoked section 230(c)(2)(B) as immunization against liability.[79]

Zango was the first time that the Ninth Circuit grappled with immunity under section 230(c)(2)(B) and is still one of the only cases throughout the circuit courts to construe this rarely-invoked subsection with some depth.[80] The Ninth Circuit focused mainly on the issue of "who" i.e., *who* was entitled to protection under Section 230 and whether immunity extended to a security software provider like Kaspersky.[81] The Ninth Circuit looked to the statute's plain language and congressional goals to conclude that the statute immunized a provider of internet security software under section 230(c)(2)(B) because they provided users with the tools to filter or screen potential malware-carrying programs, which is plainly protected under the statute.[82]

But the Ninth Circuit declined to answer questions such as "what," "why," and "how," i.e., *what* type of material may be flagged for users by security software providers, *why* may a security provider flag software, and *how far* does the scope of the immunity extend? Specifically, *Zango* raised the question of what type of material may be flagged when it asked the Ninth Circuit to define the scope of "otherwise objectionable" material.[83] On the other side, Kaspersky implored the Ninth Circuit to answer the question of why material may be flagged, arguing that section 230(c)(2)(B) should have an *implicit* good faith requirement that requires software providers invoking immunity under section 230(c)(2)(B) to act in good faith, as is required under section 230(c)(2)(A).[84]

Both of these questions were left largely unanswered by the Ninth Circuit. While the district court in *Zango* plainly concluded that "[b]y its own terms . . . Section 230(c)(2)(B) has no good faith requirement,"[85] the Ninth Circuit appeared to leave this question open for later determination. Specifically, the Ninth Circuit seemed to agree with the district court that section 230(c)(2)(B) does not include a good faith requirement as written, recognizing

[78] *Id.*

[79] *Id.* at 1172 (noting that Zango, Inc. brought claims against Kaspersky for tortious interference with contractual rights or business expectancy, trade libel, and unjust enrichment).

[80] *Id.* at 1174–75.

[81] *Id.* at 1173.

[82] *Id.*

[83] *Id.* at 1178 n.1.

[84] *Id.*

[85] Zango, Inc. v. Kaspersky Lab, Inc., No. C07-0807, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007).

that "[f]or present purposes, we note that subparagraph (B) comes with only one constraint: the protection afforded extends only to providers who 'enable or make available to . . . others' the technical means to restrict access to material that either the user or the provider deems objectionable."[86] But the Ninth Circuit declined to decide whether section 230(c)(2)(B) imposes an implicit good faith requirement, since the parties failed to properly raise the argument.[87]

The concurring opinion by Judge Fisher provided an answer to the above-question of "why" by expressing the need for an implicit good faith requirement read into section 230(c)(2)(B) and warning that without such a requirement, immunity may be extended to conduct that Congress did not intend to immunize.[88] Judge Fisher also addressed the question of "what," cautioning that "otherwise objectionable" material is an "unbounded catchall phrase" that may extend immunity to conduct that Congress did not intend to immunize.[89]

Finally, Judge Fisher predicted that "under the generous coverage of § 230(c)(2)(B)'s immunity language, a blocking software provider might abuse that immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material 'otherwise objectionable.'"[90] Judge Fisher's prescient concurring opinion proved to be accurate, as a decade later this same court, the Ninth Circuit, considered whether a security software that flagged software for allegedly anti-competitive reasons is entitled to immunity under section 230(c)(2)(B).

II. THE DECISION: ENIGMA SOFTWARE GROUP USA, LLC V. MALWAREBYTES, INC.[91]

More than a decade later, the Ninth Circuit heeded its own warning in *Zango*, explaining that "[w]e did not hold . . . that the immunity was limitless."[92] Instead, the Ninth Circuit relied heavily on congressional intent to ignore the plain language of

[86] Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1177 (9th Cir. 2009) (citing 47 U.S.C. § 230(c)(2)(B)).

[87] *Id.* ("To the extent that Zango in reply raises a different issue—whether subparagraph (B), which has no good faith language, should be construed implicitly to have a good faith component like subparagraph (A) explicitly has—the argument is waived.").

[88] *Id.* at 1179 (Fisher, J., concurring).

[89] *Id.* at 1178 (explaining that extending immunity under the "literal terms" of the statute could pose serious problems in the future).

[90] *Id.*

[91] 946 F.3d 1040 (9th Cir. 2019).

[92] *Id.* at 1045.

the statute and become one of the rare decisions that limited the scope of immunity under Section 230.

A. The Facts

Malwarebytes, Inc. ("Malwarebytes") is a security software firm that provides internet users with a filtering tool against security threats and unwanted programs on their computer.[93] Specifically, Malwarebytes identifies potentially harmful internet content and sends users a pop-up alert to warn them of a potential security risk.[94] This pop-up alert allows users to either block the potentially harmful content or proceed.[95] Similarly, Enigma Software Group ("Enigma") also provides security software that enables users to filter out security threats, thus making the two entities direct competitors.[96]

The animus between Malwarebytes and Enigma began in 2016, when Malwarebytes began classifying Enigma's software products as "threatening or unwanted" programs to its users.[97] As a result, users with Malwarebytes security software who tried to download Enigma's security software were alerted about Enigma's security risk—an alert which Enigma considered inaccurate, since its software was allegedly "legitimate, highly regarded, and [not a] security threat."[98] Consequently, Enigma brought four civil liability claims against Malwarebytes.[99] In response, Malwarebytes moved to dismiss for failure to state a claim, asserting that it was immune from liability under section 230(c)(2)(B).[100]

B. The District Court

At the district court level, Malwarebytes contended that its case was "indistinguishable" from *Zango*, and it was thus entitled to immunity under section 230(c)(2)(B).[101] Enigma, however, advanced three main arguments to demonstrate that its case was

[93] *Id.* at 1047.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*; Enigma Software Grp. USA LLC v. Malwarebytes Inc., No. 17-CV-02915, 2017 WL 5153698, at *1 (N.D. Cal. Nov. 7, 2017).

[98] *Enigma*, 946 F.3d at 1048.

[99] *Id.* (internal quotation marks omitted). Enigma alleged three state-law claims and one federal claim. *Id.* The first state-law claim alleged deceptive business practices by Malwarebytes, in violation of New York General Business Law § 349. *Id.* The second and third state-law claims accused Malwarebytes of tortious interference with business and contractual relations, in violation of New York common law. *Id.* The federal claim was for Malwarebytes's allegedly false descriptions of Enigma's product under the Lanham Act. *Id.*

[100] *Id.* at 1048.

[101] *Enigma*, 2017 WL 5153698, at *2.

distinguishable from the Ninth Circuit's opinion in *Zango*.[102] The district court ultimately agreed with Malwarebytes, holding that it was immunized against Enigma's claims.[103]

First, Enigma advanced an ejusdem generis argument to show that its flagged software did not fall into the statute's enumerated categories of material to which the immunity applies.[104] Specifically, the statute requires that the material be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or *otherwise objectionable*" to afford liability to the provider.[105] Enigma argued that its software did not fall under the statute's broad "otherwise objectionable" catch-all because its security software is "not remotely related to the [other] content categories."[106] However, the court quickly disposed of this argument and clarified that the Ninth Circuit in *Zango* clearly held that immunity under section 230(c)(2)(B) applies to material that *the provider* deems objectionable, including potential malware.[107] Thus, if Malwarebytes subjectively designated Enigma's software as malware, it was properly within the scope of "otherwise objectionable" material.[108] The court emphasized that such an interpretation aligns with the plain language of the statute, reasoning that Malwarebytes, the provider, exercised its discretion to determine that the material was objectionable and was thus entitled to immunity.[109]

Second, Enigma argued for an additional hurdle to Malwarebytes's immunity. Specifically, Enigma proposed an *implied* good faith requirement within the statute and contended that Malwarebytes was only entitled to immunity under section 230(c)(2)(B) if it acted in good faith.[110] Once again, the court disagreed with Enigma's assertion, stating explicitly that subsection (B) does not contain a good faith requirement, and reasoning that Congress acted intentionally in its inclusion of a good faith requirement in subsection (A), and its exclusion in subsection (B).[111] In particular, the court focused on subsection (B)'s clear cross-reference to subsection (A) regarding the *types* of material to which immunity applies, but its omission of any

[102] *Id.* at *2–3.
[103] *Id.* at *3–4.
[104] *Id.* at *2.
[105] 47 U.S.C. § 230(c)(2)(A) (emphasis added).
[106] *Enigma*, 2017 WL 5153698, at *2.
[107] *Id.* at *3.
[108] *Id.*
[109] *Id.* at *3–4.
[110] *Id.* at *3.
[111] *Id.*

similar reference to the good faith language in subsection (A).[112] Because of this clear statutory landscape, the court reasoned that Congress decidedly chose to omit a good faith requirement, concluding that the court need not consider whether Malwarebytes acted in good faith for the purposes of deciding whether it was entitled to immunity.[113]

Finally, unrelated to *Zango*, Enigma contended that its Lanham Act claim rendered Malwarebytes ineligible for immunity due to the statute's intellectual property exception.[114] But the court again disagreed, explaining that the Lanham Act contains two parts,[115] and since Enigma's complaint did not allege an intellectual property claim, Malwarebytes' immunity did not fall within the statute's intellectual property exception.[116] After denying Enigma's arguments, the district court held that Malwarebytes was entitled to immunity and granted its motion to dismiss.[117]

C. The Ninth Circuit: A Reversal

The Ninth Circuit, however, disagreed with the district court's dismissal and reversed and remanded the case.[118] Declaring this case an issue of first impression because the two parties were direct competitors, the Ninth Circuit narrowed the provider's discretion in deciding what material is "otherwise objectionable": the Ninth Circuit held that this broad catch-all does not include software that the provider finds objectionable for anticompetitive reasons.[119]

In its initial overview, the Ninth Circuit agreed with the district court opinion, recognizing that the provision establishes a subjective standard whereby the internet provider subjectively decides what online material is "otherwise objectionable."[120] Though the Ninth Circuit also initially acknowledged that Section 230 has a "broad recognition of immunity," it then emphasized that the immunity was not limitless.[121]

[112] *Id.*

[113] *Id.*

[114] *Id.*; *see also* 47 U.S.C. § 230(e)(2).

[115] *Enigma*, 2017 WL 5153698, at *3 (explaining that the Lanham Act addresses two distinct claims: trademark infringement and unfair competition).

[116] *Id.*

[117] *Id.* at *4.

[118] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1054 (9th Cir. 2019), *rev'g*, 2017 WL 5153698 (N.D. Cal. Nov. 7, 2017).

[119] *Id.* at 1045.

[120] *Id.* at 1044.

[121] *Id.* at 1045.

After explaining the history and policy goals of Section 230, the Ninth Circuit considered whether section 230(c)(2) immunizes blocking and filtering decisions that are driven by anticompetitive conduct.[122] The court looked to three district court decisions that previously narrowed the scope of immunity,[123] reasoning that these decisions were "persuasive" and noting that other courts interpreting *Zango* provided unlimited immunity which "stretched our opinion . . . too far."[124]

The court validated its authority to question Malwarebytes' determination of what content to block by explaining that *Zango* only addressed *who* may be entitled to immunity under Section 230, but did not address *what* type of material may be flagged as objectionable nor *why* it may be flagged under Section 230.[125] Thus, the court explained that this case properly provided the opportunity to address what limitations exist for a provider's blocking decisions.[126]

The court clarified the parties' positions on this first issue as follows. In its appeal, Enigma argued that Section 230 does not provide immunity for blocking decisions driven by anticompetitive reasons.[127] On the other side, Malwarebytes contended that it was entitled to immunity regardless of any anticompetition motives, due to the broad catch-all of "otherwise objectionable."[128] Without addressing the district court's discussion of the statute's plain language, the Ninth Circuit rejected Malwarebytes' position, reasoning that "it appears contrary to the [Communications Decency Act's] history and purpose."[129]

Instead, the court concluded that section 230(c)(2) does not immunize blocking and filtering decisions that are driven by anticompetitive motives.[130] To support its conclusion, the court leaned heavily into policy arguments.[131] Specifically, the court pointed to the congressional goals articulated in the statute, explaining "Congress said it gave providers discretion to identify objectionable content in large part to protect competition, not suppress it . . . Congress wanted to encourage the development of

[122] *Id.* at 1046–47, 1050.

[123] *See* Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 881, 884 (N.D. Cal. 2015); *see also* Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011); *see also* Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014).

[124] *Enigma*, 946 F.3d at 1050.

[125] *See id.* at 1049.

[126] *Id.* at 1050.

[127] *Id.*

[128] *Id.*

[129] *Id.* at 1050–51.

[130] *Id.* at 1051.

[131] *See id.* at 1050–51.

filtration technologies, not to enable software developers to drive each other out of business."[132]

The court also explained that allowing software providers to block content for anticompetitive reasons would lessen user control and create disincentives to the development of new filtering technology, which would purportedly run counter to Congress's explicit policy goals within the statute.[133] Thus, the court rejected Malwarebytes' position and refused to extend immunity.[134]

Next, the court considered Enigma's renewed ejusdem generis argument that the phrase "otherwise objectionable" only extends to sexual or violent online material.[135] The court quickly rejected Enigma's position, agreeing with the district court that malware could be within the scope of objectionable material, so long as it is not classified as such for anticompetitive reasons.[136]

Lastly, the court considered Enigma's assertion that its claim for false advertising, technically codified under the Lanham Act, falls within Section 230's exception to immunity for intellectual property claims.[137] The court again agreed with the district court, holding that the intellectual property carve-out was inapplicable since, although the Lanham Act deals with intellectual property, not all claims brought under the Lanham Act involve intellectual property.[138] Accordingly, the court held that false advertising claims do not involve intellectual property rights, and thus, Section 230's intellectual property exception does not apply to Enigma's false advertising claims.[139] For the foregoing reasons, the Ninth Circuit reversed the district court's dismissal and remanded for further proceedings.[140]

The dissent, however, disagreed with the majority's limitation on the scope of immunity afforded under Section 230.[141] While largely agreeing with the majority's policy arguments, Judge Rawlinson's dissent reasoned that the majority's reliance on policy "cannot be squared" with the broad language of the statute.[142]

[132] *Id.* at 1051.

[133] *Id.*; *see also* 47 U.S.C. § 230(b)(3)–(4).

[134] *Enigma*, 946 F.3d at 1051.

[135] *Id.* at 1051–52.

[136] *Id.* A recent article by Adam Candeub and Eugene Volokh closely examines the meaning of "otherwise objectionable" in this statute, arguing that this catch-all category only refers to material that is regulated by other sections of the Communications Decency Act. *See* Adam Candeub & Eugene Volokh, *Interpreting 47 U.S.C. § 230(C)(2)*, 1 J. FREE SPEECH L. 175, 180–83 (2021).

[137] *Enigma*, 946 F.3d at 1052–54.

[138] *Id.* at 1052–53.

[139] *Id.* at 1053.

[140] *Id.* at 1054.

[141] *Id.* (Rawlinson, J., dissenting).

[142] *Id.*

Moreover, Judge Rawlinson explained that the majority's holding conflicted with the precedent set forth in *Zango*, where the Ninth Circuit previously explained that the broad language of the Act is consistent with the Congressional goals for immunity.[143] The dissent aptly noted that "[t]he majority's real complaint is not that the district court construed the statute too broadly, but that the statute is written too broadly. However, that defect . . . is one beyond our authority to correct."[144]

D. The Supreme Court Denies Certiorari

After the Ninth Circuit's decision, Malwarebytes promptly petitioned for certiorari to the Supreme Court, which had never previously interpreted this provision.[145] Numerous briefs were filed in support of Malwarebytes, including briefs from cybersecurity experts,[146] a non-profit civil liberties organization,[147] and a non-partisan technology think-tank,[148] demonstrating the technology community's concern over this outlier decision. However, the Supreme Court denied certiorari, leaving Malwarebytes to defend the action on remand without the benefit of Section 230 immunity.[149]

Interestingly, in support of the Court's decision to deny certiorari, Justice Thomas issued a statement addressing the Ninth Circuit's decision.[150] Justice Thomas—who has historically rejected the consideration of legislative intent, legislative history, and sources outside of the text when engaging in statutory construction—rightly criticized courts that have "departed from the most natural reading of the text" and "filter[ed] their decisions through the policy argument" to grant immunity to internet providers under Section 230.[151] Yet the Ninth Circuit, by

[143] *Id.* at 1054–55.

[144] *Id.* at 1054.

[145] Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020).

[146] *See* Brief of Amici Curiae Cybersecurity Experts in Support of Petitioner at 1, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020) (No. 19-1284), 2020 WL 3316789, at *1.

[147] *See* Brief of Electronic Frontier Foundation As Amicus Curiae in Support of Petitioner at 1, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020) (No. 19-1284), 2020 WL 2770278, at *1.

[148] *See* Brief of Techfreedom as Amicus Curiae in Support of Petitioner at 1–2, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020) (No. 19-1284), 2020 WL 3316788, at *1–2.

[149] *See Malwarebytes*, 141 S. Ct. at 13.

[150] *See id.*

[151] *See id.* at 16, 18; *see also* Judge H. Brent McKnight, *The Emerging Contours of Justice Thomas's Textualism*, 12 REGENT U.L. REV. 365, 366 (1999); *see also* Nancie G. Marzulla, *The Textualism of Clarence Thomas: Anchoring The Supreme Court's Property Rights Jurisprudence to the Constitution*, 10 AM. U.J. GENDER SOC. POL'Y & LAW 351, 351–52 (2002).

Justice Thomas' own admission, relied heavily on policy arguments to deny immunity in this case, doing exactly what Justice Thomas cautioned against in the Court's statement.[152] Thus, by declining to grant certiorari, Justice Thomas and the Supreme Court allowed policy arguments to prevail over the statutory text.[153]

E. The Battle Continues: A Return to the District Court and Ninth Circuit

After the Supreme Court denied certiorari, the case was remanded to the United States District Court for the Northern District of California, where Malwarebytes was ultimately granted a motion for dismissal.[154] Facing the same four claims as in Enigma's earlier complaint,[155] the district court found that Enigma failed to allege the requisite elements of its various claims.[156]

Specifically, Malwarebytes' labeling of Enigma's software as "threats" and "PUPs"[157] were non-actionable, subjective *opinions* rather than false statements of fact.[158] Thus, Enigma's first claim, a violation of the Lanham Act, failed because a false statement of fact is a requisite element of the claim.[159] Enigma's second claim, a violation of New York state law for deceptive acts and unlawful business practices, similarly failed because "an opinion that is not actionable under the Lanham Act is also not actionable under [state law]."[160]

[152] *See Malwarebytes*, 141 S. Ct. at 13, 15.

[153] *See id.* at 13–14. Justice Thomas' desire to narrow the scope of Section 230 immunity has continued. In March 2022, the Supreme Court denied certiorari to another case involving subsection (c)(1) of the provision. *See* Doe v. Facebook, Inc., 142 S. Ct. 1087, 1089 (2022). In his statement respecting the denial, Justice Thomas stated:

> Here, the Texas Supreme Court recognized that '[t]he United States Supreme Court—or better yet, Congress—may soon resolve the burgeoning debate about whether the federal courts have thus far correctly interpreted section 230.' Assuming Congress does not step in to clarify § 230's scope, we should do so in an appropriate case.

Id. at 1088. (citation omitted).

[154] *See* Enigma Software Group USA LLC v. Malwarebytes Inc., No. 17-CV-02915, 2021 WL 3493764, at *1, *3 (N.D. Cal. Aug. 9, 2021).

[155] Enigma filed suit alleging (1) violation of § 43(a) of the Lanham Act; (2) violation of New York General Business Law § 349; (3) tortious interference with contractual relations; and (4) tortious interference with business relations. *See id.* at *9–*10.

[156] *See id.* at *11.

[157] "PUP" refers to a potentially unwanted program which is akin to junkware on a computer. *See* Wendy Zamora, *What is a PUP?–How to Avoid Potentially Unwanted Programs*, MALWAREBYTES LABS, http://blog.malwarebytes.com/101/2016/02/how-to-avoid-potentially-unwanted-programs/ [http://perma.cc/6Z64-AMBX] (Sept. 14, 2021).

[158] *See Enigma*, 2021 WL 3493764, at *9.

[159] *See id.*

[160] *See id.* at *10.

Third, Enigma's tortious interference with contractual relations claim was unsuccessful because Enigma "fail[ed] to identify a specific contractual obligation with which Malwarebytes interfered" and because Enigma "fail[ed] to adequately plead that Malwarebytes engaged in any independently wrongful act which interfered with a specific contractual obligation under its at-will agreements with users."[161] Thus, Enigma's tortious interference claim was similarly dismissed.[162]

Finally, Enigma's fourth claim for tortious interference with business relations was dismissed because Enigma failed to allege any intentional, wrongful conduct designed to disrupt a business relationship by Malwarebytes, which is a required element of the claim.[163] As a result, Enigma's claims were dismissed without leave to amend.[164]

Unfortunately for Malwarebytes, Enigma has already filed its appeal, meaning that Malwarebytes will be forced to return to the Ninth Circuit yet again, and this time without any discussion of Section 230 immunity.[165]

III. Implications

A. Practical Consequences

Without Section 230 immunity, Malwarebytes has been forced to defend a five-year court battle that isn't over yet. While Section 230's role in the case has ended, the Ninth Circuit's "terrible"[166] decision has permanently cracked the armor of immunity under section 230(c)(2)(B).

For instance, the litigation expenses spent by Malwarebytes over the last five years just to achieve dismissal—expenses which only continue to increase as Enigma remains committed to this fight—undermines Congress' express policy goal of promoting the development of the Internet by subjecting providers like Malwarebytes and others to costly and burdensome litigation.[167] This result is exactly why, by the Ninth Circuit's own admission, courts have consistently extended broad immunity under Section 230, explaining that "[S]ection 230 must be interpreted to protect

[161] *Id.*

[162] *Id.* at 10.

[163] *Id.* at 10–11.

[164] *Id.* at 11.

[165] *See Enigma Software Grp. USA, LLC v. Malwarebytes, Inc.*, No. 21-16466 2021 WL 3493764, (9th Cir. Sept. 7, 2021).

[166] *Terrible Ninth Circuit Ruling, supra* note 51.

[167] *See id.*

websites not merely from ultimate liability, but from having to fight costly and protracted legal battles."[168]

Indeed, as the leading Section 230 scholar Eric Goldman has cautioned, "[w]hen judges reject a defendant's motion to dismiss based on immunity and then reject the plaintiff's claim at a later procedural stage, they risk undercutting the immunity's principal benefit of fast, cheap, and reliable defense wins."[169] In fact, Goldman has proposed removing the "good faith" requirement from Section 230 entirely, reasoning that it "invites judicial confusion and increases the chances that both parties will incur more adjudication costs only to reach the same result: a prevailing defendant."[170]

Further, this decision will also likely cause security software providers to be more conservative in their filtering decisions to avoid liability and litigation like Malwarebytes has faced.[171] This is perhaps the most significant and troubling policy implication of this case—and one that the Ninth Circuit failed to recognize in its lengthy policy considerations. Namely, the Ninth Circuit's decision in *Enigma* defeats the very objectives that Section 230 was enacted to address. Congress created this statute as a direct legislative response to *Stratton Oakmont* because legislators were concerned about the chilling of self-regulation after holding a website liable for user conduct.[172] But *Enigma* now holds Malwarebytes liable for user conduct based on users deciding to filter out Enigma software. Thus, security software providers are now incentivized *not* to flag potentially harmful programs, for fear of litigation based on their users' ultimate filtering decisions. In other words, providers are right back where they started before the Communications Decency Act, facing the very dilemma about content moderation that the Act was enacted to address more than twenty years ago.

Further, the decision could have a chilling effect on the innovation of security software, as software firms now need to spend resources assessing litigation risks associated with developing security software.[173] Since security software must continuously adapt to the evolution of malware itself, a more

[168] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008); *see also* Levitt v. Yelp! Inc. (Nos. C-10-1321 EMC, C-10-2351 EMC), 2011 WL 5079526, at *8 (N.D. Cal. Oct. 26, 2011) ("The Ninth Circuit has made it clear that the need to defend against a proliferation of lawsuits, regardless of whether the provider ultimately prevails, undermines the purpose of section 230.").

[169] *See Online User Account Termination*, *supra* note 51, at 671.

[170] *Id.*

[171] *See* Szewczyk et al., *supra* note 34.

[172] *See* Bolson, *supra* note 32, at 5.

[173] *See* Szewczyk et al., *supra* note 34.

conservative approach to blocking could present serious data privacy implications for businesses and personal users alike.[174] Such an outcome hinders the express policy goal of "promot[ing] the continued development of the Internet" by impairing innovation and user safety.[175]

B. Judicial Consequences: A Clear Split in Federal and State Court

Not only does the Ninth Circuit's ruling weaken Section 230 immunity, but it also creates inconsistent outcomes for Malwarebytes outside of the Ninth Circuit. Further, the ruling has created a clear split between California state and federal courts.

Specifically, in *PC Drivers Headquarters, LP v. Malwarebytes, Inc.* ("*PC Drivers*"), Malwarebytes faced a similar suit in Texas district court after labeling one of PC Drivers' software as a PUP to users.[176] Malwarebytes asserted immunity under section 230(c)(2)(B) and, unlike the Ninth Circuit, the district court in Texas refused to read an implicit "good faith" requirement into subsection (B).[177] The court echoed the language from the district court in *Enigma*, reiterating that Congress could have easily included a good faith requirement in section 230(c)(2)(B) if it intended to, as evidenced by the fact that it included this requirement in section 230(c)(2)(A), but not section 230(c)(2)(B).[178] Thus, the court concluded that PC Drivers' claims were barred by section 230(c)(2), leaving Malwarebytes with an entirely different outcome than it received in the Ninth Circuit, solely due to differing interpretations of section 230(c)(2)(B) immunity.[179]

Additionally, just weeks after the *Enigma* decision was issued by the Ninth Circuit, a California superior court explicitly declined to follow the ruling.[180] The court in *Prager Univ. v. Google LLC* ("*Prager*") reasoned that the majority in *Enigma* ignored the plain language of the statute and improperly read a good faith limitation into section 230(c)(2)(B).[181] The court

[174] *See id.*

[175] 47 U.S.C. § 230(b)(1).

[176] PC Drivers Headquarters, LP v. Malwarebytes, Inc., No. 1:18-CV-234-RP, 2018 WL 2996897 at *1 (W.D. Tex. 2018).

[177] *See id.* at *2–3.

[178] *Id.* at *3.

[179] *See id.* at *4.

[180] Prager Univ. v. Google LLC, No. 19CV340667, 2019 WL 8640569, at *1 (Cal. Super. Ct. Nov. 19, 2019).

[181] *Id.* at *10. The court expressed strong disagreement with the Ninth Circuit's decision in *Enigma*, "who ignore[d] the plain language of the statute by reading a good faith limitation into Section 230(c)(2)(B)." *Id.*

explained that a critical distinction between 230(c)(2)(A) and 230(c)(2)(B) is that subsection (A), which contains a good faith requirement, contemplates website providers that *unilaterally* restrict access to online material, whereas subsection (B), which does not have a good faith requirement, allows users to *voluntarily* restrict access to material.[182] The court criticized the idea of adding a good faith requirement into subsection (B), firmly holding that such an addition is "contrary to the plain language of the statute."[183]

As Malwarebytes explained in its petition for certiorari to the Supreme Court, these conflicting approaches to section 230(c)(2)(B) in the *Enigma*, *PC Drivers*, and *Prager* cases have opened "a rift between state and federal fora in the technology center of the Nation," adding that "plaintiffs now have every incentive to bring suit in federal courts," thereby opening the door for forum shopping.[184]

IV. THE NINTH CIRCUIT: DEFYING THE RULES OF STATUTORY CONSTRUCTION

In addition to these troubling practical implications, the ways in which the Ninth Circuit arrived at its decision were flawed for several significant reasons.

A. Plain Language

First, the well-established rules of statutory construction provide that courts must start with the operative text of the statute, and if the statutory text is plain and unambiguous, then the inquiry into statutory interpretation begins and ends with the language of the statute itself.[185] In *Enigma*, the dissent reminded the majority of the Supreme Court's often-cited directive that

[182] *Id.*

[183] *Id.* at *11.

[184] Petition for a Writ of Certiorari, at *4, *20, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 592 U.S. 1 (2020) (No. 19-1284), 2020 WL 2494604.

[185] *See* Robinson v. Shell Oil Co., 519 U.S. 337, 340 (1997) ("Our inquiry must cease if the statutory language is unambiguous."); *see also* King v. Burwell, 576 U.S. 472, 486 (2015) ("If the statutory language is plain, we must enforce it according to its terms."); Barnhart v. Sigmon Coal Co., 534 U.S. 438, 462 (2002) ("When the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'"); ABNER J. MIKVA & ERIC LANE, AN INTRODUCTION TO STATUTORY INTERPRETATION AND THE LEGISLATIVE PROCESS 24 (1997) (explaining that the plain meaning rule is not an optional canon of construction and instead is "the constitutionally compelled starting place for any statutory construction," adding that alternative "tools of interpretation are only applicable when the plain meaning rule fails to provide the answer.").

courts "must presume that a legislature says in a statute what it means and means in a statute what it says there."[186]

While the Ninth Circuit initially acknowledged that the statute plainly permits providers like Malwarebytes to block material that the provider subjectively considers objectionable, the Ninth Circuit ignored the district court's clear holding that Section 230(c)(2)(B) does not have a good faith requirement and its refusal to read an implicit good faith requirement.[187] Instead, the Ninth Circuit improperly departed from the plain language and proceeded to its view of the statute's history and policy, reasoning that Congress' unusual step of including express policy goals justified the court's reliance on policy.[188]

Pointing to its own earlier warnings in *Zango*, the court explained that an overly expansive interpretation of the broad term "objectionable" would allow providers to classify content as objectionable for anticompetitive reasons.[189] The court reasoned that such an outcome would run counter to Congress' express policy goals.[190] While the Ninth Circuit's policy determinations have merit if Malwarebytes was seeking immunity under section 230(c)(2)(A), the Ninth Circuit's policy rationale reveals a misunderstanding of the facts at hand. For example, the court justified its holding by stating that:

> Interpreting the statute to give providers unbridled discretion to block online content would . . . enable and potentially motivate internet-service providers to act for their own, and not the public, benefit. 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.[191]

However, the Ninth Circuit failed to recognize that the district court did not grant Malwarebytes "unbridled discretion" to block online content. According to the district court's fact-finding, Malwarebytes identified potentially harmful software and notified users of the perceived threat, asking the *user* whether they wanted to remove the content from their computer.[192] In other words, it was the users that were choosing whether to heed Malwarebytes' warning and block the content or otherwise proceed with the Enigma

[186] Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1055 (9th Cir. 2019) (Rawlinson, J., dissenting) (quoting Conn, Nat'l Bank v. Germain, 503 U.S. 249, 253–54 (1992)).

[187] *See id.* at 1045, 1054.

[188] *See id.* at 1044–47.

[189] *Id.* at 1045, 1047.

[190] *Id.* at 1044–47.

[191] *Id.* at 1051.

[192] *Enigma*, 2017 WL 5153698, at *1.

software. Thus, it was the users, not the provider, that were exercising their "unbridled discretion" in blocking content, fulfilling Congress' express policy goal of maximizing user control, not running contrary to policy as the Ninth Circuit improperly stated.

Further, as the Ninth Circuit recognized earlier in *Zango*, users are *choosing* to install and utilize security software like Malwarebytes.[193] As Goldman explains in the context of *Enigma*, "if Malwarebytes' users aren't happy with its blocking function, the users can uninstall Malwarebytes and adopt Enigma instead. This means consumers are empowered to override Malwarebytes' decisions."[194] In other words, the user conduct that Enigma based its claims on actually furthered Congress' desire for increased user control.

Additionally, even if the Ninth Circuit's policy determinations were correct, it is well-established that courts are to enforce a statute as it is written, even if doing so undercuts Congressional purpose or policy.[195] The Ninth Circuit seemed to justify its policy-focused decision because Congress wrote this statute at a time when it was unable to identify all of the types of internet material that may be encompassed by this statute, thus opting for broad language.[196] But as the Supreme Court has recognized, broad language, such as the phrase "otherwise objectionable," does not render a statute's text ambiguous.[197] In fact, the Supreme Court has previously noted that congressional objectives may actually require broad, general language in a statute and that it is Congress, not the courts through the guise of statutory ambiguity, that must define the statute's limits.[198]

Even within the context of Section 230, lower courts have recognized that narrowing the scope of broad statutory language within this particular statute is for Congress, not courts, to

[193] *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1176 (9th Cir. 2009).

[194] *Terrible Ninth Circuit Ruling, supra* note 51.

[195] *See* Shambie Singer, *§46:1: The Plain Meaning Rule*, *in* SUTHERLAND STATUTORY CONSTRUCTION (7th ed., 2020) (explaining that if the statute's language is plain and unambiguous, then the "the sole function of the courts is to enforce it according to its terms"); *see also* Baker Botts L.L.P. v. Asarco LLC, 576 U.S. 121, 134–35 (2015). Even Justice Thomas has pointed out that the Supreme Court "lack[s] the authority to rewrite the statute" by stating: "Our job is to follow the text even if doing so will supposedly undercut a basic objective of the statute." *Id.*; *see also* Lamie v. U.S. Trustee, 540 U.S. 526, 538 (2004) ("Our unwillingness to soften the import of Congress' chosen words even if we believe the words lead to a harsh outcome is longstanding. It results from 'deference to the supremacy of the Legislature, as well as recognition that Congressmen typically vote on the language of a bill.'").

[196] *See Enigma*, 946 F.3d at 1051.

[197] *See, e.g.*, Diamond v. Chakrabarty, 447 U.S. 303, 315 (1980).

[198] *See id.*

remedy.[199] Indeed, as the dissent wisely pointed out, even if the statute is written too broadly, it was beyond the Ninth Circuit's authority to correct.[200] Further, more than 20 years since the statute's enactment, Congress has still declined to correct the broad scope of the term "otherwise objectionable," revealing its preference to leave the broad catch-all as written.

Under the cardinal rules of statutory construction, the Ninth Circuit should not have proceeded to policy considerations if the statutory text was clear. The court improperly jumped to these policy considerations without considering that the resulting narrow interpretation was incompatible with the operative statutory text. By doing so, the Ninth Circuit overreached its judicial authority.

B. Express Inclusion, Implied Exclusion

The Ninth Circuit's next misstep demonstrates its fundamental misunderstanding and misreading of the statute's plain text. After highlighting the policy considerations, the court clarified its view of "the legal question" in this case: whether section 230(c)(2) immunizes blocking and filtering decisions that are driven by anticompetitive animus.[201] By posing the legal question as such and determining the scope of liability under section 230(c)(2), the court failed to recognize that 230(c)(2)(A) and 230(c)(2)(B) are separate subsections, one with a good faith requirement, and one without.[202] Thus, the court collapsed the key distinction between the two unique subsections and read an implicit good faith requirement into subsection (B).

Generally, where Congress includes particular language in one section of a statute but omits it in another section of the same statute, it is presumed that Congress has acted intentionally in its disparate inclusion or exclusion.[203] The distinction in statutory language reveals Congress' well-considered position that the two statutes carry different meaning and purpose.[204] Further, courts are reluctant to add statutory requirements that conflict with the

[199] *See* Barrett v. Rosenthal, 146 P.3d 510, 529 (Cal. 2006) (Moreno, J., concurring) ("Although there may be a considerable gap between the specific wrongs Congress was intending to right in enacting the immunity at issue here and the broad statutory language of that immunity, that gap is ultimately for Congress, rather than the courts, to bridge.").

[200] *Enigma*, 946 F.3d at 1054.

[201] *Id.* at 1045.

[202] *Id.*

[203] *See, e.g.*, Keene Corp. v. U.S., 508 U.S. 200, 207–08 (1993).

[204] *See, e.g.*, Digital Realty Trust, Inc. v. Somers, 138 S. Ct. 767, 777 (2018) ("[W]hen Congress includes particular language in one section of a statute but omits it in another[,] . . . this Court presumes that Congress intended a difference in meaning.").

plain language of the statute, especially when Congress has included such requirements in other areas of the same statute.[205] As the Supreme Court has explained, "[w]e do not lightly assume that Congress has omitted from its adopted text requirements that it nonetheless intends to apply, and our reluctance is even greater when Congress has shown elsewhere in the same statute that it knows how to make such a requirement manifest."[206]

In this case, the Ninth Circuit explained that *Zango* only addressed *who* may be entitled to immunity under Section 230, yet the court used this case to answer *what* type of material may be blocked as objectionable and *why* it may be blocked under section 230(c)(2).[207] While the court's determination that subsection (A) does not immunize anticompetitive conduct is logical and convincing, Malwarebytes was entitled to protection under section 230(c)(2)(B), just like the security software provider in *Zango*. Thus, the court's dual inquiry into *what* material and *why* it is deemed objectionable was improper under section 230(c)(2)(B) because there is no good faith language in subsection (B) as written.

Also, to justify its decision to limit the statute's broad scope of immunity, the court cited three cases that have previously narrowed the scope of material deemed objectionable.[208] Yet, these cases considered the scope of immunity under section 230(c)(2)(A), whereas *Enigma* considered the scope of immunity under section 230(c)(2)(B). By finding these cases comparable, the court once again conflated the fundamental distinction between subsection (A) and subsection (B), a distinction which renders these cited precedents inapposite to the case at hand.

For example, in *Song fi Inc. v. Google, Inc.* ("*Song fi*") and *Holomaxx Technologies. v. Microsoft Corp.* ("*Holmaxx*"), the district courts considered *why* the providers removed the material to determine whether the providers rightly deemed the

[205] *See, e.g.*, Russello v. United States, 464 U.S. 16, 23 (1983) (finding that if Congress had intended to add restrictions, it would have done so, as evidenced by its restricting language in the immediately following subsection, but concluding that Congress did not write the statute that way, refusing to conclude "that the differing language in the two subsections has the same meaning in each" because the Court "would not presume to ascribe this difference to a simple mistake in draftsmanship").

[206] Jama v. Immigr. & Customs Enf't, 543 U.S. 335, 341 (2005); *see also* Romag Fasteners, Inc. v. Fossil, Inc. 140 S. Ct. 1492, 1495 (2020) ("[T]his Court [does not] usually read into statutes words that aren't there. It's a temptation we are doubly careful to avoid when Congress has (as here) included the term in question elsewhere in the very same statutory provision.").

[207] *See Enigma*, 946 F.3d at 1049–50.

[208] *See id.* at 1050 (citing Song fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 883 (N.D. Cal. 2015), Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104–05 (N.D. Cal. 2011), and Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014)).

material "otherwise objectionable."[209] These were proper inquiries, since these providers were required to act in good faith in their determination of what material was "objectionable" under section 230(c)(2)(A).

Here, however, Malwarebytes was merely providing users with technology to filter material, instead of actually filtering objectionable material as in *Song fi* and *Holomaxx*. Thus, under subsection (B), the court's analysis should have stopped after determining whether the material was the type of material that may be blocked. The court should not have looked any further into the reasons why the provider blocked the material and whether the provider's determination was made in good faith.

While it is true that the language in section 230(c)(2)(B) explicitly refers to section 230(c)(2)(A) in determining the *types* of material that may be removed, subsection (B) does not require that providers act in good faith in their determination. As Malwarebytes contended, a provider would still be entitled to immunity regardless of bad faith, anticompetitive motives based on the statute as written.[210] The dissent in *Enigma* made this point, explaining that "the majority holds that the criteria for blocking online material may not be based on the identity of the entity that produced it. Unfortunately, however, that conclusion cannot be squared with the broad language of the Act."[211]

By citing *Song fi* and *Holomaxx* and inquiring into the anticompetitive motives of Malwarebytes in its determination of whether the content was "objectionable," the court impermissibly collapsed the distinction between subsection (A) and subsection (B), added an implied requirement of good faith in Malwarebytes' determination of what content is objectionable, and violated the statutory principle that, where Congress has employed a term in one place and excluded it in another, it should not be implied where excluded.[212]

C. Statutory Exceptions

The Ninth Circuit's conclusion that a provider may not designate online material as "otherwise objectionable" for anticompetitive reasons also violates a significant line of precedent involving statutory exceptions. As written, Congress

[209] *See Song fi*, 108 F. Supp. 3d at 884; *Holomaxx*, 783 F. Supp. 2d at 1104–05.

[210] *See Enigma*, 938 F.3d at 1036.

[211] *Id.* at 1040 (Rawlison, J., dissenting) (citation omitted).

[212] *See, e.g.*, FTC v. Simplicity Pattern Co., 360 U.S. 55, 66–67 (1959); *see also* Stewart v. Ragland, 934 F.2d 1033, 1041 (9th Cir. 1991) ("When certain statutory provisions contain a requirement and others do not, we should assume that the legislature intended both the inclusion and the exclusion of the requirement.").

enumerates five exceptions from immunity where providers are not shielded from liability by Section 230.[213]

Generally, where Congress has explicitly carved out certain exceptions within a statute, courts do not have the authority to create additional exceptions.[214] Indeed, the long-standing rule of *expressio unius est exclusio alterius*, meaning the express mention of one thing excludes all others, assumes that if Congress intended to include other exceptions, it would have expressed them in the statute.[215]

Courts, including the Supreme Court,[216] First Circuit,[217] Fifth Circuit,[218] Sixth Circuit,[219] and Eleventh Circuit,[220] have heeded this doctrine and refused to read additional statutory exceptions where Congress has explicitly provided others within the statute.

[213] The five exceptions are (1) criminal law, (2) intellectual property law, (3) state law, (4) communications privacy law, and (5) sex trafficking law. Thus, website providers cannot be granted immunity against these types of claims. *See* 47 U.S.C. § 230(e).

[214] *See, e.g.*, United States v. Johnson, 529 U.S. 53, 58 (2000).

[215] *See, e.g.*, Clifton Williams, *Expressio Unius Est Exclusio Alterius*, 15 MARQ. L. REV. 191, 193 (1931) (discussing State v. Regents of Univ. of Wis., 54 Wis. 159 (1882)) ("The student wanted to make additional exceptions to the statute, but the Court rejected the idea, stating that the enumeration of certain exceptions in the Statute excluded all other exceptions, and applied the rule . . . ."); *see also* Eliot v. Eliot, 51 N.W. 81, 81 (1892).

> It is fair to assume that, had the legislature intended other restrictions upon the right of action, it would have expressed the same in the statute. *Expressio unius est exclusio alterius*. In our opinion, it is not permissible for the court to interpolate conditions and exceptions and restrictions upon the right of action, not expressed therein, and which would thwart the plain legislative intention on the subject.

Id. (emphasis in original).

[216] *See, e.g.*, United States v. Johnson, 529 U.S. 53, 58 (2000) ("When Congress provides exceptions in a statute, it does not follow that courts have authority to create others. The proper inference, and the one we adopt here, is that Congress considered the issue of exceptions and, in the end, limited the statute to the ones set forth."); *see also* Law v. Siegel, 571 U.S. 415, 424 (2014) ("The Code's meticulous . . . enumeration of exemptions and exceptions to those exemptions confirms that courts are not authorized to create additional exceptions."); Rowe v. N.H. Motor Transp. Ass'n, 552 U.S. 364, 374 (2008) (explaining that when a statute explicitly lists a set of exceptions, Congress is unlikely to have intended additional implicit exceptions).

[217] *See, e.g.*, Dickow v. United States, 654 F.3d 144, 152 (1st Cir. 2011) ("[T]he explicit listing of exceptions . . . 'indicate[d] . . . that Congress did not intend courts to read other unmentioned, open-ended, 'equitable' exceptions into the statute.'") (quoting United States v. Brockamp, 519 U.S. 347, 352 (1997)).

[218] *See, e.g.*, *In re* Mirant Corp., 378 F.3d 511, 522 (5th Cir. 2004) ("Obviously, Congress knew how to draft an exclusion . . . when it wanted to; its failure to do so in this instance indicates that Congress intended that.") (quoting NLRB v. Bildisco & Bildisco, 465 U.S. 513, 522–23 (1984)).

[219] *See, e.g.*, County of Oakland v. Fed. Hous. Fin. Agency, 716 F.3d 935, 940 (6th Cir. 2013) ("Accordingly, because the statutes are clear, we are not in a position to second-guess Congress and create a new exception in the statute . . . .").

[220] *See, e.g.*, Allstate Life Ins. Co. v. Miller, 424 F.3d 1113, 1116 n.3 (11th Cir. 2005) ("[W]here the legislature has included certain exceptions . . . the doctrine of *expressio unis* [sic] *est exclusio alterius* counsels against judicial recognition of additional exceptions.") (emphasis in original).

But in the *Enigma* case, the Ninth Circuit disregarded the doctrine of *expressio unius est exclusio alterius* by creating a new statutory exception under the guise of "otherwise objectionable" language. Specifically, by explicitly holding that section 230(c)(2) did not immunize blocking decisions involving anticompetitive conduct, the court potentially carved out a new exception to Section 230's immunity.[221]

This weakens Section 230's power because security software firms like Enigma that have their content blocked by a user utilizing competing filtering software, like Malwarebytes, can now simply allege anticompetitive conduct—even if the content by a competitor was filtered for legitimate reason—and the provider will be unable to rely on Section 230 immunity.[222] Indeed, as Malwarebytes asserted in its petition for certiorari, the Ninth Circuit "elevated its own policy considerations over Congress's chosen words. It did exactly what [the Supreme Court] has admonished: it rewrote the statute to add a new exception from immunity" for allegations of anticompetitive conduct.[223]

Interestingly, Congress recently proposed a sixth exception for Section 230, where the statute's immunity would not extend to website providers who fail to report suspicious online

[221] *See* Eric Goldman, *As Expected, Malwarebytes Defeats Enigma's Lawsuit Without Section 230's Help*, TECH. & MKTG. L. BLOG (Sept. 5, 2021), http://blog.ericgoldman.org/archives/2021/09/as-expected-malwarebytes-defeats-enigmas-lawsuit-without-section-230s-help.htm#:~:text=Malwarebytes%20classified%20Enigma's%20software%20as,)(2)(B)%20grounds [http://perma.cc/4ETR-J6RB].

> [T]he Ninth Circuit created a new workaround to Section 230 based on anticompetitive animus. This workaround is completely undefined–is it coextensive with antitrust law, or does apply when competitors have anticompetitive "intent" even if their actions don't constitute an antitrust violation? The Ninth Circuit dodged this critical issue. . . .
>
> Should we applaud the Ninth Circuit for so carefully policing the boundaries of Section 230's immunities, or should we criticize them for unnecessarily swiss-cheesing Section 230?

Id.

[222] *See Terrible Ninth Circuit Ruling*, *supra* note 51.

> [E]ven when a software vendor actually directly competes with the anti-threat vendor, it might still be appropriate to block it. Unfortunately, the anti-threat software industry has too many sleazy players who are really in the scareware or adware business. When anti-threat vendors' direct competitors are also threats to consumers, the court's standards virtually ensure that Section 230(c)(2) won't be available.

Id.

[223] Brief of Techfreedom as Amicus Curiae in Support of Petitioner, Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (No. 19-1284), 2020 WL 3316788, at *6.

transmissions related to terrorism.[224] This recent proposal demonstrates Congress' willingness to craft new statutory exceptions into Section 230. Moreover, Congress' failure to propose a statutory exception for anticompetitive practices suggests that Congress does not intend for such conduct to be excluded from the scope of Section 230's liability.

D. Alternative Course of Action

Ultimately, the Ninth Circuit's conclusion that immunity under Section 230 should not extend to anticompetitive conduct has merit. Nevertheless, instead of crafting a new carve-out from immunity that Congress did not intend, the Ninth Circuit should have followed the First Circuit and Second Circuit's approach to problematic policy outcomes. Specifically, the court should have applied the statute as written, extended immunity to Malwarebytes, and allowed Congress to amend the statute to address anticompetitive behavior, as it did to address terrorism after *Force v. Facebook* ("*Force*") and sex-trafficking claims after *Jane Doe No. 1 v. Backpage.com* ("*Backpage*").[225]

In *Force*, the Second Circuit extended immunity to Facebook, despite Facebook's failure to remove online content that facilitated and celebrated terrorist attacks in Israel.[226] While the majority remained committed to a plain reading of the statute and did not discuss the troubling policy implications of its decision, the dissent denounced the outcome, writing "we today extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another."[227] But, after a lengthy discussion, the dissent still conceded that "[w]hether, and to what extent, Congress should allow liability for tech companies that encourage terrorism, propaganda, and extremism is a question for legislators, not judges."[228]

Similarly, in *Backpage*, a website provider was shielded from civil liability under Section 230 against three victims of sex-trafficking who brought suit.[229] While the First Circuit conceded "[t]his is a hard case . . . the law requires that we, like the court below, deny relief to plaintiffs whose circumstances evoke outrage," it applied the statute as written and extended immunity

[224] See Something, Say Something Online Act of 2021, S. 27, 117th Cong. § 4 (2021).

[225] *See* Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 23 (1st Cir. 2016); Force v. Facebook, Inc., 934 F.3d 53, 81 (2d Cir. 2019).

[226] *See id.* at 57.

[227] *Id.* at 77 (Katzmann, C.J., concurring in part and dissenting in part).

[228] *Id.* at 88.

[229] *See* 817 F.3d at 12.

to the website provider, despite the negative policy implications that followed.[230] The First Circuit justified its decision by stating that "Congress did not sound an uncertain trumpet when it enacted the [Communications Decency Act], and it chose to grant broad protections to internet publishers," adding that, "the remedy is through legislation, not through litigation."[231]

Despite the highly undesirable policy implications that resulted in *Backpage* and *Force*, the First and Second Circuits adhered to the well-respected canons of statutory interpretation, refused to depart from the statute's plain text in favor of compelling policy considerations, and criticized the results in its opinion, passing the onus to correct these problems where it belongs: on Congress.

Indeed, this approach is exactly what the Supreme Court has prescribed, as Justice Sotomayor has previously warned, "it would be improper to allow policy considerations to undermine the American Rule."[232] Moreover, Justice Gorsuch has explained "[a]s these things go . . . the place for reconciling competing and incommensurable policy goals like these is before policymakers. This Court's limited role is to read and apply the law those policymakers have ordained . . . ."[233]

Further, the First and Second Circuit's approach was successful, as Congress took immediate legislative action after *Backpage* and *Force* by promptly introducing new limitations on immunity into Section 230.[234] As one scholar noted, "[t]he *Backpage* cases demonstrated a flaw in the system, and Congress acted to solve that specific problem. That is precisely how the legislative process should work."[235]

If its sister circuits were willing to follow the statute's plain language even in the presence of sex-trafficking survivors and victims of international terrorism, the Ninth Circuit, too, should have been steadfast in its refusal to depart from the plain text for computer software providers. In short, the Ninth Circuit should have followed the statute as written and called for Enigma's remedy to come through legislation, not litigation.

[230] *Id.* at 15.

[231] *Id.* at 29.

[232] Baker Botts L.L.P. v. Asarco LLC, 536 U.S. 121, 135 (2015) (Sotomayor, J., concurring in part and concurring in the judgment).

[233] Romag Fasteners, Inc. v. Fossil, Inc., 140 S. Ct. 1492, 1497 (2020).

[234] *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. § 2 (2017); *see also* See Something, Say Something Online Act of 2021, S. 27 117th Cong. § 4 (2021).

[235] KOSSEFF, *supra* note 1, at 280.

CONCLUSION

At first glance, the Ninth Circuit's determination in *Enigma*—that website providers are not entitled to Section 230 immunity for anticompetitive conduct—may seem like a logical limitation on the safe harbor's broad scope. But a closer examination of the facts reveals the fundamental flaws of this decision, including a fatal misreading of the statute that conflates two unique shields of immunity and an emphasis on flawed policy considerations that now impose an implicit good faith requirement where Congress decidedly omitted one. The decision has already caused a judicial split that the Supreme Court stood unwilling to address. In doing so, the Court allowed the Ninth Circuit to usurp congressional power by improperly narrowing the statute and crafting a sixth carve-out from immunity, despite Congress' demonstrated willingness to do so in other contexts.

Above all, this decision has troubling implications for website users and providers, alike. In the area of security software, users will be forced to navigate an internet with more conservative security decisions and less filtering. At the same time, security software providers encounter an all too familiar dilemma: the exact dilemma that Congress sought to rectify when it created this safe harbor over twenty years ago. Namely, providers have two options: allow users to filter and face liability, *or* remove filtering tools and avoid liability, but leave harmful content online.