No. 17-17351

IN THE

United States Court of Appeals

FOR THE NINTH CIRCUIT

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

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

BRIEF OF *AMICUS CURIAE* INTERNET ASSOCIATION IN SUPPORT OF PETITION FOR REHEARING AND REHEARING EN BANC

Lauren Gallo White
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (415) 947-2000
Facsimile: (415) 947-2099
lwhite@wsgr.com

Brian M. Willen
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
1301 Avenue of the Americas
40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899
bwillen@wsgr.com

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, the undersigned counsel for amicus curiae certifies that the Internet Association is a trade association representing leading global internet companies on matters of public policy. Internet Association does not have any parent corporations and does not issue stock.

Dated: November 7, 2019

By: /s/ Brian M. Willen
Brian M. Willen
Attorney for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF IDENTITY OF AMICUS CURIAE, ITS INTEREST IN THE CASE, AND ITS AUTHORITY TO FILE

The Internet Association ("IA") represents over 40 of the world's leading internet companies. IA's mission is to foster innovation, promote economic growth, and empower people through a free and open internet.

IA has a strong interest in the proper application of Section 230 of the Communications Decency Act ("CDA"). IA members host enormous amounts of material uploaded by users, and they rely on Section 230 to protect their everyday operations, including their content-moderation efforts. IA submits this brief because it is concerned that the panel's decision threatens those self-regulatory practices and will harm the quality of online platforms and the experiences of those who use them.

All parties have consented to the filing of this brief. No party authored this brief, in part or in whole, and no party or counsel for any party—or any person other than amicus, its members, and its counsel—contributed any money intended to fund preparing or submitting this brief.

SUMMARY OF ARGUMENT

Section 230(c)(2) of the CDA provides vital protections for the self-regulatory efforts of online services and software providers. This provision immunizes actions that online platforms and their users take to block, filter, or avoid material that they consider inappropriate or objectionable. Relying on this immunity, service providers have developed a wide array of tools that allow families and others to avoid content that, for one reason or another, they would rather not see. That includes tools specifically covered by Section 230(c)(2)(B)—such as YouTube's Restricted Mode, Twitter's Block feature, and Reddit's Quarantine function—which empower users to make their own decisions about whether, when, and how to restrict access to material they might find offensive. All of this helps realize the animating vision of Section 230—to encourage voluntary self-regulation in lieu of heavy-handed government censorship.

In this case, however, over a forceful dissent from Judge Rawlinson, the panel put these valuable content-moderation efforts at risk. The panel's misguided ruling exposes online services to lawsuits that Section 230 is supposed to stop in their tracks and opens the door to new attacks on self-regulatory tools that help make online communities safer and more accommodating. If allowed to stand, the panel opinion will undermine a core purpose of Section 230, with far-reaching consequences for online service providers and their users. Rehearing is required to correct this mistake.

Three aspects of the majority's decision especially concern IA and its members. ***First***, the panel improperly imported a motive-based good-faith limitation into Section 230(c)(2)(B). As explained in Appellee's rehearing petition, that defies fundamental rules of statutory interpretation and collapses an important distinction between subsection (c)(2)(A), which includes an express "good faith" requirement, and subsection (c)(2)(B), which conspicuously omits one.

Second, by uncritically accepting what appears from the opinion to be Appellant's bare allegations of anticompetitive animus, the panel's decision threatens to make it all too easy for plaintiffs to plead around Section 230(c)(2)(B). That result is squarely at odds with this Court's decisions in *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc), and *Kimzey v. Yelp!, Inc.*, 836 F.3d 1263 (9th Cir. 2016). Those cases make clear that because Section 230 protects service providers against protracted legal battles (not just ultimate liability), the immunity cannot be defeated at the pleading stage with conclusory assertions. The panel's contrary approach puts the content-moderation decisions of online providers and users at risk of "death by ten thousand duck-bites," *Roommates.com*, 521 F.3d at 1174, opening the door to costly litigation for any plaintiff willing to make even threadbare allegations of improper motive. That subverts Congress's goal of encouraging and removing disincentives for the development and use of filtering technologies.

Third, the majority's dictum that the "criteria for blocking online material must be based on the characteristics of the online material, *i.e.*, its content, *and not on the identity of the entity that produced it*," Dkt. 42-1 ("Slip Op.") at 10 (emphasis added), is particularly troubling. While perhaps unintended by the panel, this stray statement could be applied in ways that would further undermine the very practices that Section 230 was intended to protect. Online service providers and their users routinely make moderation decisions that apply to entities or individuals, rather than just isolated pieces of content. That happens, for example, when a provider terminates a user's account or when users deploy tools like Twitter's Block feature to filter content from certain other users. These measures are a vital part of online self-regulation and are covered by any coherent reading of Section 230(c)(2). The panel's ambiguous language threatens to arbitrarily limit the ability of platforms and users to protect themselves against abusive, offensive, or problematic accounts or users. At a minimum, therefore, the Court should grant rehearing to correct (or strike) the panel's errant dicta.

ARGUMENT

I. SECTION 230(c)(2) PROVIDES VITAL PROTECTIONS FOR SELF-REGULATION BY ONLINE SERVICES AND THEIR USERS

Congress enacted Section 230, in significant part, "to encourage interactive computer services and users of such services to self-police the Internet for obscenity and other offensive material, so as to aid parents in limiting their children's access to such material." *Batzel v. Smith*, 333 F.3d 1018, 1028 (9th Cir. 2003). The statute establishes as the "policy" of the United States "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," and "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." 47 U.S.C. § 230(b)(3), (4). To accomplish this, Section 230(c)(2) provides robust immunity both for online service providers' decisions to directly restrict access to objectionable material and for the actions they take to make available to others the "technical means to restrict access" to such content. *Id*. § 230(c)(2)(A), (B).

This approach facilitates meaningful *private* content-regulation that helps protect internet users from potentially objectionable or harmful material, while avoiding *government* regulation of online speech that may offend the First Amendment. *Accord Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 885 (1997).

Section 230 forged a middle way between heavy-handed state censorship and an internet with no meaningful content moderation, where objectionable material of all kinds may make online activity unsafe for children, sensitive users, or vulnerable groups. *See Batzel*, 333 F.3d at 1028. "Rather than imposing penalties on Internet posters and their service providers," the proponents of Section 230 "argued that it would be more effective and fair to allow individuals and companies to set their own standards." Jeff Kosseff, The Twenty-Six Words That Created the Internet 63 (2019); *see e.g.*, 141 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox) ("We want to help [the evolution of technology] … by saying Government is going to get out of the way and let parents and individuals control it rather than Government doing that job for us.").

The user-empowering "technical means" protected by subsection (c)(2)(B) are integral to this approach. This immunity enabled the development of all manner of tools that help users protect themselves against material they may find offensive or otherwise may not wish to see. The malware-blocking software at issue in this case only scratches the surface. IA's members have made available numerous tools that fall squarely within what Congress imagined with subsection (B). For example:

- YouTube's Restricted Mode provides an option for users (including parents, libraries, and schools) to select a more limited YouTube experience that screens out videos that may be inappropriate for some

audiences, including videos depicting alcohol, descriptions of violence, or political conflicts.[1]

- Twitter's Mute and Block tools allow users to stop seeing Tweets and other content from those whom they may dislike or find objectionable.[2]

- On Reddit—a network of user-run communities—content regulation depends heavily on volunteer user moderators using tools supplied by Reddit.[3] Moderators in each community set rules that fit their specific needs, which they enforce via a suite of tools that includes means for:

  - Manually removing individual rule-breaking posts or comments;

  - Automatically removing individual posts or comments according to moderator-configurable rules (*e.g.*, if the submission includes a particular word, or if the submitter is not on the moderators' list of pre-approved contributors); and

  - Temporarily or permanently banning rule-breaking users from posting or commenting in the community.[4]

- Reddit gives its users tools for choosing whether to see material labeled "NSFW" (not safe for work). NSFW labels can be applied not only to

---

[1] *See* Disable or enable Restricted/Safe Mode, YOUTUBE, https://support.google.com/youtube/answer/174084?co=GENIE.Platform%3DDesktop&hl=en.

[2] *See* How to mute accounts on Twitter, TWITTER, https://help.twitter.com/en/using-twitter/twitter-mute; How to block accounts on Twitter, TWITTER, https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts.

[3] More than 99% of the pieces of content removed from Reddit in 2018 were removed by volunteer user moderators using Reddit-provided tools. *See* Transparency Report 2018, REDDIT, https://www.redditinc.com/policies/transparency-report-2018.

[4] *See* Moderation Tools – overview, REDDIT, https://mods.reddithelp.com/hc/en-us/articles/360008425592-Moderation-Tools-overview.

individual pieces of content, but also to user profiles and entire communities.[5]

- Reddit also lets its users control (via an opt-in mechanism) whether they see material from "quarantined" communities, which contain material that average users may find highly offensive or upsetting.[6]

The efficacy of tools like these depends on service providers and users having the freedom to determine for themselves what material they find objectionable. Content that may be objectionable for some platforms, communities, or users might not be objectionable for others. Section 230 accommodates this reality by eschewing a one-size-fits-all approach and instead imposing a flexible, subjective standard.

Through subsection (c)(2)(B) in particular, Congress wanted to protect—with a broad immunity that does not depend on a finding of good faith—filtering technologies that allow individual providers and users to make nuanced, context-specific moderation decisions based on their own sensibilities and standards. *See* Kosseff, The Twenty-Six Words at 64 (explaining that the framers of Section 230 "hoped that the services would be free to set their own standards for user content" and believed the market "would encourage the companies to develop conduct codes

[5] *See* Post Actions – Lock, OC, NSFW, and Spoiler, REDDIT, https://mods.reddithelp.com/hc/en-us/articles/360025119251-Post-Actions-Lock-OC-NSFW-and-Spoiler; Community settings, REDDIT, https://mods.reddithelp.com/hc/en-us/articles/360022692051-Community-settings.

[6] *See* Quarantined Subreddits, REDDIT, https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/quarantined-subreddits.

that are most appropriate for their audiences"); 141 Cong. Rec. H8470 (statement of Rep. Cox) ("This technology is very quickly becoming available, and in fact every one of us will be able to tailor what we see to our own tastes."). In short, the statute allows service providers "to establish standards of decency without risking liability for doing so." *Green v. AOL*, 318 F.3d 465, 472 (3d Cir. 2003).

II. THE PANEL OPINION MISINTERPRETS SECTION 230(c)(2)(B) AND CONFLICTS WITH THIS COURT'S CASES

The panel's opinion threatens to undermine the self-regulatory efforts that Section 230 is supposed to facilitate. From IA's perspective, there are three key problems with the ruling that warrant rehearing. *First*, the panel's core holding effectively reads into Section 230(c)(2)(B) a good faith requirement that Congress omitted. *Second*, the panel's uncritical acceptance of Appellant's allegations makes it far too easy for plaintiffs to evade Section 230 immunity at the pleading stage and contradicts the approach this Court took in *Roommates* and *Kimzey*. *Third*, the panel's suggestion in dicta that Section 230(c)(2) may not apply to blocking decisions based "on the identity of the entity," Slip Op. at 10, could be misapplied to exclude a host of important content-moderation efforts that restrict or limit objectionable *users* or *entities*, rather than just individual pieces of content.

A. The Panel Improperly Engrafted A Good Faith Requirement Into Section 230(c)(2)(B) That Congress Omitted

The majority held that Section 230(c)(2)(B) does not protect "blocking and filtering decisions that are driven by anticompetitive animus." Slip Op. at 16. The panel thus adopted a purpose-based test: filtering decisions that otherwise would be covered by the immunity are excluded because the service provider (or user) allegedly acted with an improper motive or purpose. In so doing, the panel effectively read into Section 230(c)(2)'s "otherwise objectionable" language a new good faith requirement.

This holding defies core principles of statutory interpretation. "'Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.'" *Asarco LLC v. Atl. Richfield Co.*, 866 F.3d 1108, 1118–19 (9th Cir. 2017) (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983)). That rule should have controlled this case. Section 230(c)(2) contains two subsections, which provide distinct but related immunities. The first (subsection (A)) includes an express "good faith" requirement; while subsection (B) conspicuously excludes any reference to good faith. This omission creates a strong presumption that this immunity does *not* turn on any consideration of good faith—whether in the form of an anticompetitive motive or otherwise.

This rule applies with particular force here, as Congress had good reason to omit a good faith requirement from subsection (c)(2)(B). Subsection (A) covers direct blocking or filtering by interactive computer service providers—situations where providers act unilaterally to protect themselves or their users from objectionable material. *See Batzel*, 333 F.3d at 1030 n.14. But subsection (B) only applies where service providers make blocking tools available to users, who must independently and affirmatively decide to use those tools. Here, blocking does not occur unilaterally; it instead requires cooperation between a service provider and a third party. *Id*. at 1029 ("Some blocking and filtering programs depend on the cooperation of website operators and access providers who label material that appears on their services.").

In that scenario, Congress logically concluded that it was unnecessary to include a good faith requirement or for courts to inquire about the service providers' motives. The user's independent choice operates as a check on providers' decisions about what material should be filtered or blocked. Indeed, this Court's decision in *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009), recognized this vital element of user choice under 230(c)(2)(B): "If a Kaspersky user (who has bought and installed Kaspersky's software to block malware) is unhappy with the Kaspersky software's performance, he can uninstall Kaspersky and buy blocking

software from another company that is less restrictive or more compatible with the user's needs." *Id.* at 1177.

In engrafting an extra-textual motive requirement into 230(c)(2)(B), the panel overlooked the important difference between the two provisions and lost sight of how subsection (B) is supposed to apply. Under that provision as written—and as applied in *Zango*—what matters is simply whether the technical means provided restricts access to material that a service provider or user subjectively "considers" to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c)(2)(A); *accord Zango*, 568 F.3d at 1173 ("We think the statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user or the provider deems objectionable."); *see also* Slip Op. at 25 (Rawlinson, J., dissenting). Inquiries into the "real" purpose of the blocking are unnecessary—and inappropriate. The panel's departure from the plain language of the statute and the approach followed in *Zango* warrants rehearing.

B. The Panel Opinion Conflicts With This Court's Cases By Allowing Vague Allegations Of Animus To Defeat Section 230 Immunity

Exacerbating these problems is the panel's uncritical acceptance of seemingly vague allegations of anticompetitive motive to defeat a motion to dismiss based on Section 230. *See* Slip Op. at 20 ("Enigma alleges, however, that its programs 'pose

no security threat' and that Malwarebytes's justification for blocking these 'legitimate' and 'highly regarded' programs was a guise for anticompetitive animus."). The majority's approach further conflicts with this Court's precedents and undermines a core aim of Section 230.

This first conflict is with *Roommates*. Sitting en banc, this Court held that Section 230 protects "websites not merely from ultimate liability, but from having to fight costly and protracted legal battles." *Roommates.com*, 521 F.3d at 1175. Under this rule, courts must "aim to resolve the question of § 230 immunity at the earliest possible stage of the case." *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 255 (4th Cir. 2009) (citing *Roommates.com*). The panel ignored this principle. It allowed Enigma to overcome Section 230 and move this case into discovery—with all the "costly and protracted" battles that entails—based on what seems from the opinion to be little more than conclusory allegations of animus. That defies this Court's admonition that "close cases . . . must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites." *Roommates.com*, 521 F.3d at 1174.

The panel's treatment of Enigma's allegations is also directly contrary to this Court's decision in *Kimzey v. Yelp*. That case involved the immunity under Section 230(c)(1), which applies only where the service provider was not responsible for the "creation or development" of the material at issue. 836 F.3d at 1266 (citation

omitted). As here, the plaintiff tried to "plead around" Section 230 "to advance the same basic argument that the statute plainly bars." *Id*. But this Court "decline[d] to open the door to such artful skirting of the CDA's safe harbor provision." *Id*. Instead, after carefully scrutinizing the allegations in the complaint, the Court held that Kimzey had failed to "'plead facts tending to demonstrate that the . . . review was not, as is usual, authored by a user.'" *Id.* at 1268 (quoting *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014)) (alteration in original). *Kimzey* thus made clear that a robust application of the requirement of plausible factual allegations is needed to ensure that plaintiffs cannot evade Section 230 immunity with "creative pleading," *id*. at 1265–66:

> We have no trouble in this case concluding that threadbare allegations of fabrication of statements are implausible on their face and are insufficient to avoid immunity under the CDA. . . . Were it otherwise, CDA immunity could be avoided simply by reciting a common line that user-generated statements are not what they say they are.

Id. at 1268–69 (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

Here, the panel allowed precisely the kind of evasion of Section 230 that *Kimzey* rejected. Through creative pleading, Enigma offered what the panel treated as a largely unadorned claim of anticompetitive animus. Such allegations are not uncommon: parties upset that their material has been blocked or filtered will often assert—without any support or factual basis—that the decision was driven by some kind of animus. Following *Kimzey*, the panel should have responded to such

allegations by confirming that Section 230 cannot be so readily avoided—that "the immunity in the CDA is broad enough to require plaintiffs alleging such a theory to state the facts plausibly suggesting" that Malwarebytes did not actually consider Enigma's software objectionable. *Id.* at 1269. But the panel failed even to cite *Kimzey*, much less apply its rigorous approach.

This conflict underscores the need for rehearing. As this Court observed in *Kimzey*: "It cannot be the case that the CDA and its purpose of promoting the free exchange of information and ideas over the Internet could be so casually eviscerated." *Id.* (quotation marks omitted). Indeed, if plaintiffs can sidestep Section 230 at the pleading stage in this way, the immunity loses much of its value. *Accord Nemet*, 591 F.3d at 255 (recognizing that Section 230 immunity from suit "is effectively lost if a case is erroneously permitted to go to trial") (citation omitted). Based on barebones allegations, service providers (and even users) may be threatened with expensive and time-consuming litigation to defend their self-regulatory efforts—efforts that happen constantly, given the massive scale of online communications. As much as the actual risk of liability, such litigation burdens significantly raise the costs of engaging in self-regulation, and some providers may find that the risk is simply not worth it. That, of course, is the opposite of how Section 230 is supposed to work. *See* Eric Goldman, Online User Account Termination and 47 U.S.C. § 230(c)(2), 2 U.C. Irvine L. Rev. 659, 671 (2012)

(explaining that one of the "principal benefit[s]" of Section 230 is the promise "of fast, cheap, and reliable defense wins").

In short, the panel's approach will *discourage* rather than "encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools," 47 U.S.C. § 230(b)(3), and it will *create* rather than "remove disincentives for the development and utilization of blocking and filtering technologies," *id*. § 230(b)(4). Rehearing should be granted to bring this case in line with this Court's cases and ensure that Section 230 continues to play the role that Congress intended.

III. LOOSE DICTA IN THE PANEL OPINION THREATENS ESPECIALLY FAR-REACHING CONSEQUENCES FOR ONLINE SERVICES AND USERS

Beyond all the problems discussed above, the panel's opinion also includes dicta that could have even more pernicious consequences for online self-regulation.

Early in its opinion, the majority opines that under Section 230(c)(2), the "criteria for blocking online material must be based on the characteristics of the online material, *i.e.*, its content, and not on the identity of the entity that produced it." Slip Op. at 10. This passage, which is not expressly tethered to the allegations of anticompetitive motive, "cannot be squared with the broad language of the Act," *id*. at 25 (Rawlinson, J., dissenting), or its purpose of removing disincentives for efforts to protect internet users. The panel's dicta could be read to suggest that Section

230(c)(2) does not apply where a decision to restrict content or apply a blocking tool focused on an objectionable *user* or *account*, rather than on individual pieces of objectionable content. Such a limitation has no basis in the statute and would create serious problems for online service providers and their users.

Consistent with Section 230(c)'s broad protections, online service providers routinely identify potentially harmful content based on its source. Anti-spam software often relies on the behaviors exhibited by users,[7] and computer security programs enable users to block entire web pages known to distribute malware.[8] Likewise, online platforms (including IA members) have terminated the accounts of neo-Nazi groups like The Daily Stormer—and other entities whose messages do not fit within their values and rules.[9] Even more directly relevant here, the user-empowerment tools discussed above, such as Twitter's blocking and muting features, allow users to block or restrict content from specific user-accounts they

[7] Yiqun Liu, et al., User behavior oriented web spam detection, in Proc. of 17th International Conference on World Wide Web 2008, WWW'08, Apr. 21, 2008 – Apr. 25, 2008, Beijing, China, 1039–40 (2008).

[8] Block access to malicious URLs with web reputation, TRENDMICRO, https://help.deepsecurity.trendmicro.com/Protection-Modules/Web-Reputation/ug-web-rep.html.

[9] Andrew Buncombe, Twitter deletes Daily Stormer's account amid outrage at neo-Nazi site's response to Charlottesville, INDEPENDENT (Aug. 16, 2017, 10:00 PM), https://www.independent.co.uk/news/world/americas/daily-stormer-charlottesville-twitter-accounts-deleted-heather-heyer-funeral-a7897411.html.

deem objectionable. The same is true of Reddit's quarantine device, which applies to entire communities (or "subreddits") within the larger Reddit service.

These kinds of account- or speaker-specific tools are vital for the self-regulation contemplated by Section 230. If service providers or users could only block specific items of content, the protections they offer would be materially diminished. In many cases, removing or filtering out all content from objectionable users or accounts is the best way to deal with abuse, misbehavior, or simply unwanted online interactions. That is why, for example, the government-sponsored website stopbullying.gov recommends that users "[b]lock *the person* who is cyberbullying" as a step "to [t]ake [i]mmediately" in the face of online harassment or abuse.[10]

But these protective efforts are threatened by the panel's dicta. When service providers take actions or offer tools like these, they arguably are restricting access to material at least in part based on the "identity of the entity that produced it." Slip Op. at 10. Seizing on this language, litigants may try to get around Section 230 by alleging that a service provider blocked—or enabled users to block—content because of animus toward the speaker. And lower courts bound by the panel's ruling may think (incorrectly) that they need to withhold immunity from self-regulatory

[10] Report Cyberbullying, STOPBULLYING.GOV, http://www.stopbullying.gov/cyberbullying/how-to-report/index.html.

efforts that go beyond blocking or filtering individual pieces of content. That would have calamitous consequences that have no basis in Section 230. To the contrary, such quintessential acts of self-policing are exactly the kinds of efforts to limit objectionable online material—and "to aid parents in limiting their children's access to such material"—that Section 230(c)(2) is designed to protect. *Batzel*, 333 F.3d at 1028.

Accordingly, even if the result in this case is otherwise unchanged, the majority's errant dicta should be eliminated before it is misused to strip Section 230(c)(2) immunity from a host of socially beneficial measures that protect online services and their users.

CONCLUSION

For these reasons, Appellee's petition for rehearing should be granted.

Dated: November 7, 2019

Respectfully submitted,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Brian M. Willen
Brian M. Willen
Attorney for Amicus Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

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

I am the attorney or self-represented party.

This brief contains 4,144 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated [ ].
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Brian M. Willen **Date** 11/07/2019

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

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on November 7, 2019, which will serve a notice of electronic filing on all registered users, including counsel for the parties.

Dated: November 7, 2019

/s/ Brian M. Willen
Brian M. Willen
Attorney for Amicus Curiae