

Statement of THOMAS, J.

SUPREME COURT OF THE UNITED STATES

**MALWAREBYTES, INC. v. ENIGMA SOFTWARE
GROUP USA, LLC**

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED
STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

No. 19–1284. Decided October 13, 2020

The petition for a writ of certiorari is denied.

Statement of JUSTICE THOMAS respecting the denial of certiorari.

This petition asks us to interpret a provision commonly called §230, a federal law enacted in 1996 that gives Internet platforms immunity from some civil and criminal claims. 47 U. S. C. §230. When Congress enacted the statute, most of today’s major Internet platforms did not exist. And in the 24 years since, 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.

This case involves Enigma Software Group USA and Malwarebytes, two competitors that provide software to enable individuals to filter unwanted content, such as content posing security risks. Enigma sued Malwarebytes, alleging that Malwarebytes engaged in anticompetitive conduct by reconfiguring its products to make it difficult for consumers to download and use Enigma products. In its defense, Malwarebytes invoked a provision of §230 that states that a computer service provider cannot be held liable for providing tools “to restrict access to material” that it “considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.” §230(c)(2). The Ninth Circuit relied heavily on the “policy” and “purpose” of §230 to conclude that immunity is unavailable when a plaintiff alleges anticompetitive conduct.

The decision is one of the few where courts have relied on purpose and policy to *deny* immunity under §230. But the court’s decision to stress purpose and policy is familiar. Courts have long emphasized nontextual arguments when interpreting §230, leaving questionable precedent in their wake.

I agree with the Court’s decision not to take up this case. I write to explain why, in an appropriate case, we should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms.

I

Enacted at the dawn of the dot-com era, §230 contains two subsections that protect computer service providers from some civil and criminal claims. The first is definitional. It states, “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.” §230(c)(1). This provision ensures that a company (like an e-mail provider) can host and transmit third-party content without subjecting itself to the liability that sometimes attaches to the publisher or speaker of unlawful content. The second subsection provides direct immunity from some civil liability. It states that no computer service provider “shall be held liable” for (A) good-faith acts to restrict access to, or remove, certain types of objectionable content; or (B) giving consumers tools to filter the same types of content. §230(c)(2). This limited protection enables companies to create community guidelines and remove harmful content without worrying about legal reprisal.

Congress enacted this statute against specific background legal principles. See *Stewart v. Dutra Constr. Co.*, 543 U. S. 481, 487 (2005) (interpreting a law by looking to the “backdrop against which Congress” acted). Traditionally, laws governing illegal content distinguished between

Statement of THOMAS, J.

publishers or speakers (like newspapers) and distributors (like newsstands and libraries). Publishers or speakers were subjected to a higher standard because they exercised editorial control. They could be strictly liable for transmitting illegal content. But distributors were different. They acted as a mere conduit without exercising editorial control, and they often transmitted far more content than they could be expected to review. Distributors were thus liable only when they knew (or constructively knew) that content was illegal. See, e.g., *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710, *3 (Sup. Ct. NY, May 24, 1995); Restatement (Second) of Torts §581 (1976); cf. *Smith v. California*, 361 U. S. 147, 153 (1959) (applying a similar principle outside the defamation context).

The year before Congress enacted §230, one court blurred this distinction. An early Internet company was sued for failing to take down defamatory content posted by an unidentified commenter on a message board. The company contended that it merely distributed the defamatory statement. But the company had also held itself out as a family-friendly service provider that moderated and took down offensive content. The court determined that the company's decision to exercise editorial control over some content "render[ed] it a publisher" even for content it merely distributed. *Stratton Oakmont*, 1995 WL 323710, *3–*4.

Taken at face value, §230(c) alters the *Stratton Oakmont* rule in two respects. First, §230(c)(1) indicates that an Internet provider does not become the publisher of a piece of third-party content—and thus subjected to strict liability—simply by hosting or distributing that content. Second, §230(c)(2)(A) provides an additional degree of immunity when companies take down or restrict access to objectionable content, so long as the company acts in good faith. In short, the statute suggests that 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).

This modest understanding is a far cry from what has prevailed in court. Adopting the too-common practice of reading extra immunity into statutes where it does not belong, see *Baxter v. Bracey*, 590 U. S. — (2020) (THOMAS, J., dissenting from denial of certiorari), courts have relied on policy and purpose arguments to grant sweeping protection to Internet platforms. *E.g.*, 1 R. Smolla, *Law of Defamation* §4:86, p. 4–380 (2d ed. 2019) (“[C]ourts have extended the immunity in §230 far beyond anything that plausibly could have been intended by Congress); accord, Rustad & Koenig, *Rebooting Cybertort Law*, 80 Wash. L. Rev. 335, 342–343 (2005) (similar). I address several areas of concern.

A

Courts have discarded the longstanding distinction between “publisher” liability and “distributor” liability. Although the text of §230(c)(1) grants immunity only from “publisher” or “speaker” liability, the first appellate court to consider the statute held that it eliminates distributor liability too—that is, §230 confers immunity even when a company distributes content that it *knows* is illegal. *Zeran v. America Online, Inc.*, 129 F. 3d 327, 331–334 (CA4 1997). In reaching this conclusion, the court stressed that permitting distributor liability “would defeat the two primary purposes of the statute,” namely, “immuniz[ing] service providers” and encouraging “selfregulation.” *Id.*, at 331, 334. And subsequent decisions, citing *Zeran*, have adopted this holding as a categorical rule across all contexts. See, *e.g.*, *Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F. 3d 413, 420 (CA1 2007); *Shiamili v. Real Estate Group of NY, Inc.*, 17 N. Y. 3d 281, 288–289, 952 N. E. 2d 1011, 1017 (2011); *Doe v. Bates*, 2006 WL 3813758, *18 (ED Tex., Dec. 27, 2006).

Statement of THOMAS, J.

To be sure, recognizing some overlap between publishers and distributors is not unheard of. Sources sometimes use language that arguably blurs the distinction between publishers and distributors. One source respectively refers to them as “primary publishers” and “secondary publishers or disseminators,” explaining that distributors can be “charged with publication.” W. Keeton, D. Dobbs, R. Keeton, & D. Owen, *Prosser and Keeton on Law of Torts* 799, 803 (5th ed. 1984).

Yet there are good reasons to question this interpretation.

First, Congress expressly imposed distributor liability in the very same Act that included §230. Section 502 of the Communications Decency Act makes it a crime to “knowingly . . . display” obscene material to children, even if a third party created that content. 110 Stat. 133–134 (codified at 47 U. S. C. §223(d)). This section is enforceable by civil remedy. 47 U. S. C. §207. It is odd to hold, as courts have, that Congress implicitly eliminated distributor liability in the very Act in which Congress explicitly imposed it.

Second, Congress enacted §230 just one year after *Stratton Oakmont* used the terms “publisher” and “distributor,” instead of “primary publisher” and “secondary publisher.” If, as courts suggest, *Stratton Oakmont* was the legal backdrop on which Congress legislated, *e.g.*, *FTC v. Accusearch Inc.*, 570 F. 3d 1187, 1195 (CA10 2009), one might expect Congress to use the same terms *Stratton Oakmont* used.

Third, had Congress wanted to eliminate both publisher and distributor liability, it could have simply created a categorical immunity in §230(c)(1): No provider “shall be held liable” for information provided by a third party. After all, it used that exact categorical language in the very next subsection, which governs removal of content. §230(c)(2). Where Congress uses a particular phrase in one subsection and a different phrase in another, we ordinarily presume that the difference is meaningful. *Russello v. United States*, 464 U. S. 16, 23 (1983); *cf. Doe v. America Online, Inc.*, 783

So. 2d 1010, 1025 (Fla. 2001) (Lewis, J., dissenting) (relying on this rule to reject the interpretation that §230 eliminated distributor liability).

B

Courts have also departed from the most natural reading of the text by giving Internet companies immunity for their own content. Section 230(c)(1) protects a company from publisher liability only when content is “provided by *another* information content provider.” (Emphasis added.) Nowhere does this provision protect a company that is itself the information content provider. See *Fair Housing Council of San Fernando Valley v. Rummates.Com, LLC*, 521 F. 3d 1157, 1165 (CA9 2008). And an information content provider is not just the primary author or creator; it is anyone “responsible, *in whole or in part*, for the creation or development” of the content. §230(f)(3) (emphasis added).

But from the beginning, courts have held that §230(c)(1) protects the “exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or *alter* content.” *E.g., Zeran*, 129 F. 3d, at 330 (emphasis added); cf. *id.*, at 332 (stating also that §230(c)(1) protects the decision to “edit”). Only later did courts wrestle with the language in §230(f)(3) suggesting providers are liable for content they help develop “in part.” To harmonize that text with the interpretation that §230(c)(1) protects “traditional editorial functions,” courts relied on policy arguments to narrowly construe §230(f)(3) to cover only substantial or material edits and additions. *E.g., Batzel v. Smith*, 333 F. 3d 1018, 1031, and n. 18 (CA9 2003) (“[A] central purpose of the Act was to protect from liability service providers and users who take some affirmative steps to edit the material posted”).

Under this interpretation, a company can solicit thousands of potentially defamatory statements, “selec[t] and edi[t] . . . for publication” several of those statements, add

Statement of THOMAS, J.

commentary, and then feature the final product prominently over other submissions—all while enjoying immunity. *Jones v. Dirty World Entertainment Recordings LLC*, 755 F. 3d 398, 403, 410, 416 (CA6 2014) (interpreting “development” narrowly to “preserv[e] the broad immunity th[at §230] provides for website operators’ exercise of traditional publisher functions”). To say that editing a statement and adding commentary in this context does not “creat[e] or develo[p]” the final product, even in part, is dubious.

C

The decisions that broadly interpret §230(c)(1) to protect traditional publisher functions also eviscerated the narrower liability shield Congress included in the statute. Section 230(c)(2)(A) encourages companies to create content guidelines and protects those companies that “in good faith . . . 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.” Taken together, both provisions in §230(c) most naturally read to protect companies when they unknowingly *decline* to exercise editorial functions to edit or remove third-party content, §230(c)(1), and when they *decide* to exercise those editorial functions in good faith, §230(c)(2)(A).

But by construing §230(c)(1) to protect *any* decision to edit or remove content, *Barnes v. Yahoo!, Inc.*, 570 F. 3d 1096, 1105 (CA9 2009), courts have curtailed the limits Congress placed on decisions to remove content, see *e-ventures Worldwide, LLC v. Google, Inc.*, 2017 WL 2210029, *3 (MD Fla., Feb. 8, 2017) (rejecting the interpretation that §230(c)(1) protects removal decisions because it would “swallo[w] the more specific immunity in (c)(2)”). With no limits on an Internet company’s discretion to take down material, §230 now apparently protects companies who racially discriminate in removing content. *Sikhs for Justice*,

Inc. v. Facebook, Inc., 697 Fed. Appx. 526 (CA9 2017), aff'g 144 F. Supp. 3d 1088, 1094 (ND Cal. 2015) (concluding that “any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune” under §230(c)(1)).

D

Courts also have extended §230 to protect companies from a broad array of traditional product-defect claims. In one case, for example, several victims of human trafficking alleged that an Internet company that allowed users to post classified ads for “Escorts” deliberately structured its website to facilitate illegal human trafficking. Among other things, the company “tailored its posting requirements to make sex trafficking easier,” accepted anonymous payments, failed to verify e-mails, and stripped metadata from photographs to make crimes harder to track. *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F. 3d 12, 16–21 (CA1 2016). Bound by precedent creating a “capacious conception of what it means to treat a website operator as the publisher or speaker,” the court held that §230 protected these website design decisions and thus barred these claims. *Id.*, at 19; see also *M. A. v. Village Voice Media Holdings, LLC*, 809 F. Supp. 2d 1041, 1048 (ED Mo. 2011).

Consider also a recent decision granting full immunity to a company for recommending content by terrorists. *Force v. Facebook, Inc.*, 934 F. 3d 53, 65 (CA2 2019), cert. denied, 590 U. S. — (2020). The court first pressed the policy argument that, to pursue “Congress’s objectives, . . . the text of Section 230(c)(1) should be construed broadly in favor of immunity.” 934 F. 3d, at 64. It then granted immunity, reasoning that recommending content “is an essential result of publishing.” *Id.*, at 66. Unconvinced, the dissent noted that, even if all publisher conduct is protected by §230(c)(1), it “strains the English language to say that in

Statement of THOMAS, J.

targeting and recommending these writings to users . . . Facebook is acting as ‘the *publisher* of . . . information provided by another information content provider.’” *Id.*, at 76–77 (Katzmann, C. J., concurring in part and dissenting in part) (quoting §230(c)(1)).

Other examples abound. One court granted immunity on a design-defect claim concerning a dating application that allegedly lacked basic safety features to prevent harassment and impersonation. *Herrick v. Grindr LLC*, 765 Fed. Appx. 586, 591 (CA2 2019), cert. denied, 589 U. S. ____ (2019). Another granted immunity on a claim that a social media company defectively designed its product by creating a feature that encouraged reckless driving. *Lemmon v. Snap, Inc.*, 440 F. Supp. 3d 1103, 1107, 1113 (CD Cal. 2020).

A common thread through all these cases is that the plaintiffs were not necessarily trying to hold the defendants liable “as the publisher or speaker” of third-party content. §230(c)(1). Nor did their claims seek to hold defendants liable for removing content in good faith. §230(c)(2). Their claims rested instead on alleged product design flaws—that is, the defendant’s own misconduct. Cf. *Accusearch*, 570 F. 3d, at 1204 (Tymkovich, J., concurring) (stating that §230 should not apply when the plaintiff sues over a defendant’s “*conduct* rather than for the *content* of the information”). Yet courts, filtering their decisions through the policy argument that “Section 230(c)(1) should be construed broadly,” *Force*, 934 F. 3d, at 64, give defendants immunity.

II

Paring back the sweeping immunity courts have read into §230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place. Plaintiffs still must prove the merits of their cases, and some claims will undoubtedly fail. Moreover, States and the Federal Government are free to update their liability laws to make them

more appropriate for an Internet-driven society.

Extending §230 immunity beyond the natural reading of the text can have serious consequences. Before giving companies immunity from civil claims for “knowingly host[ing] illegal child pornography,” *Bates*, 2006 WL 3813758, *3, or for race discrimination, *Sikhs for Justice*, 697 Fed. Appx., at 526, we should be certain that is what the law demands.

Without the benefit of briefing on the merits, we need not decide today the correct interpretation of §230. But in an appropriate case, it behooves us to do so.