No. ____

IN THE

Supreme Court of the United States

JOHN DOE,
Petitioner,

v.

SNAP, INC., doing business as SNAPCHAT,
L.L.C., doing business as SNAP, L.L.C.,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Fifth Circuit

PETITION FOR A WRIT OF CERTIORARI

PETER K. STRIS
STRIS & MAHER LLP
777 S. Figueroa Street, Suite 3850
Los Angeles, CA 90017

DEREK MERMAN
HEARD MERMAN LAW FIRM
4900 Fournace Place, Suite 240
Bellaire, Texas 77401

TILLMAN J. BRECKENRIDGE
COUNSEL OF RECORD
COLLEEN R. SMITH
STRIS & MAHER LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 800-6030
tbreckenridge@stris.com

Counsel for Petitioner

QUESTION PRESENTED

John Doe's high school science teacher used Snapchat when Doe was 15 years old to groom him, induce his drug abuse, and then sexually assault him. Under 47 U.S.C. Section 230(c)(1), an internet service provider cannot be treated as the "publisher" or "speaker" of information transmitted by another content provider. Doe does not seek to hold Snap liable as a publisher or speaker, but rather (1) as a host who negligently designed an environment rife with sexual predators and then lured children in, and (2) as a distributor who knew or should have known, given the technology it uses to screen content for advertisers, that Doe's teacher was using Snapchat to groom him. The question presented is:

Does 47 U.S.C. Section 230 immunize internet service providers from any suit based on their own tortious misconduct simply because third-party content is also involved?

PARTIES TO THE PROCEEDINGS

The Petitioner in this case is a John Doe plaintiff. Petitioner was the plaintiff and appellant below.[1]

The Respondent is Snap, Inc., doing business as Snapchat, L.L.C., doing business as Snap, L.L.C. It was the defendant and appellee below.

RELATED PROCEEDINGS

U.S. Court of Appeals for the Fifth Circuit:

Doe v. *Snap, Inc.*, No. 22-20543 (June 26, 2023)

U.S. District Court for the Southern District of Texas:

Doe v. *Snap, Inc.*, No. 4:22-cv-00590 (Sept. 15, 2022)

---

[1] Doe was a minor during proceedings below but has since reached the age of majority. Below, he participated through Next Friend Jane Roe, his legal guardian.

TABLE OF CONTENTS

Page

APPENDIX CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

Statutes

TABLE OF AUTHORITIES (CONTINUED)

Other Authorities

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

PETITION FOR A WRIT OF CERTIORARI

This Court already has acknowledged the question presented here is worthy of review and desperately needs it. The Court took up the question last term, but that case was not the right vehicle because the underlying claim of aiding and abetting terrorism by Facebook was not viable on its face. Here, that impediment does not exist, and the Court can provide desperately needed guidance on 47 U.S.C. § 230.

Below, seven of fifteen voting judges called for the Fifth Circuit to rehear this case en banc and revisit its faulty precedent on Section 230(c)(1). Its case law grants broad, atextual immunity to internet platforms from any claim that involves third-party created content. Falling just short of the threshold, these seven judges called on this Court to step in where they could not: "[I]t is once again up to our nation's highest court to properly interpret the statutory language enacted by Congress in" Section 230. These dissenting voices joined a growing chorus of circuit judges across the county calling for a reexamination of the proper scope of Section 230.

Congress enacted Section 230(c) to protect services' efforts to *prevent* obscenity and protect children. Under Section 230(c), a provider acting as moderator and eliminating obscene and pornographic posts does not render the provider a "publisher" or "speaker" for those or other posts. And the provider is immunized against claims by the posts' originators that it unlawfully removed their posts. That is all. It does not provide the broad immunity the Fifth Circuit found with no textual or policy basis.

The circuit courts and their judges are in disarray on the issue. The Fourth Circuit started the Courts of Appeals down the wrong path, holding that Section 230 increased protection for providers *who do nothing* to protect users. Nearly every other circuit followed along, adopting some version of broad immunity. There is a circuit conflict. The Seventh Circuit has properly applied Section 230's text and recognized that it does not grant immunity to providers who sit by and watch predators use their platforms to solicit and abuse children. After decades of lower courts expanding Section 230's protections, ten circuit judges spread across the Second, Fifth, and Ninth Circuits have now called for a course correction. But that course correction will not happen in the circuit courts. They continue to apply their wrong-headed precedents over vigorous dissents and, in this case, refused to rehear the question. Only this Court can provide the desperately need change these judges are calling for.

This case presents the perfect vehicle for this Court to intervene and properly interpret 47 U.S.C. § 230(c). Section 230 immunity is the only legal question at issue in this case, and every avenue of lower court review has been exhausted. In addition, the facts here highlight how far the lower courts have strayed from the statutory text and purpose. A teacher used Snapchat to groom Petitioner, then a 15-year-old student, induce him to drug abuse, and sexually abuse him. Snapchat was the teacher's tool of choice because its messages self-destruct moments after they are seen, destroying all evidence without any effort. Snapchat lacks safety features to prevent illicit communications between adults and minors, despite assuring parents that it has created a safe

online environment for their children. These features have, unsurprisingly, made Snapchat a haven for pedophiles and molesters.

Section 230's scope is an issue of exceptional importance. American teenagers' social media use is nearly universal. Every time a teenager refreshes a feed, he or she could be the target of online abuse. Yet social media companies are not taking reasonable and obvious steps to protect children online, and courts have applied Section 230 to cut off any means to hold them accountable. This Court's review is needed now. Further delay means further unaccountability and more tragedy, like the abuse that occurred here.

OPINIONS BELOW

The opinion of the Fifth Circuit is currently unreported and is reproduced at page 1a of the appendix to this petition ("Pet. App."). The dissent from denial of en banc review of seven out of the fifteen voting active Fifth Circuit judges is reported at 88 F.4th 1069 and reproduced at Pet. App. 41a. The decision of the district court is currently unreported and is reproduced at Pet. App. 4a.

JURISDICTION

The decision of the Fifth Circuit was entered on June 26, 2023. The order of the Fifth Circuit denying rehearing en banc was entered on December 18, 2023. Pet. App. 40a. This Court has jurisdiction under 28 U.S.C. § 1254(1). The district court had jurisdiction under 28 U.S.C. §§ 1331 and 1367(a).

STATUTORY PROVISIONS INVOLVED

47 U.S.C. § 230(c) provides:

> (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).

STATEMENT OF THE CASE

A. Statutory Background.

Congress enacted Section 230 as part of the Telecommunications Act of 1996, "a statute designed to deregulate and encourage innovation in the telecommunications industry," not the internet. *Force* v. *Facebook, Inc.*, 934 F.3d 53, 77 (2d Cir. 2019) (citing Pub. L. 104–104, § 509, 110 Stat. 56, 56, 137–39) (Katzmann, J. concurring in part, dissenting in part). In constructing the Act, "the Internet was an afterthought" and social media was unimaginable. *Id.* Facebook would not debut until 2004, eight years later, and Snapchat would not arrive until 2011, 15 years later. Mark Hall, *Facebook*, Encyclopædia Britannica, http://tinyurl.com/y9ztar76; Brian O'Connell, *History of Snapchat: Timeline and Facts*, The Street (Feb. 28, 2020), http://tinyurl.com/5n7mebf8. Around the time of Section 230's enactment, the internet had about 40 million users worldwide. *Reno* v. *ACLU*, 521 U.S. 844, 850 (1997). Now, an estimated 5.4 billion people—over half of the world's population—use it. DataReportal & Meltwater & We Are Social, *Number of internet and social media users worldwide as of January 2024 (in billions)*, Statista (Jan. 2024), http://tinyurl.com/j9hhbvcx.

Section 230(c) was aimed at protecting children from indecent online content. 141 Cong. Rec. H8468–70 (Aug. 4, 1995). Its sponsors specifically sought to prevent the effects of two New York decisions that "provide[d] a massive disincentive for the people who might best help us control the Internet" from doing so. *Id.* First, in *Cubby, Inc.* v. *CompuServe, Inc.*, 776 F. Supp. 135, 137–40 (S.D.N.Y. 1991), the court held that CompuServe, one of the first online computer services,

could not be liable for defamation as a "publisher" of a news article posted "in a publication carried on [its] computerized database." *Id.* If CompuServe were liable, it could only be as a "distributor" because it did not participate in creating or publishing the material. *Id.* But distributors only can be liable if they knew or should have known of the defamatory content. *Id.* CompuServe just provided a bulletin board for posting the material, so it could not be liable. *Id.* According to Section 230's sponsor, the fact that CompuServe avoided liability by failing to moderate content was inappropriate. 141 Cong. Rec. H8469.

Second, in *Stratton Oakmont, Inc.* v. *Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), the court held a company liable for defamation when it made a good faith attempt to monitor messages on its computer network, an act that rendered it a "publisher," rather than just a distributor. As a publisher, the company was liable for defamatory content that appeared on its services, regardless of whether the company knew about it, should have known about it, promoted it, or participated in its dissemination. *Id.* at *3–*4.

Section 230's sponsor decried these decisions as "backward" for placing "higher" liability on services that protected users by "exercis[ing] some control over offensive material," than on those who did nothing to moderate their user-created content. 141 Cong. Rec. H8470. Accordingly, the sponsors proposed Section 230(c)—entitled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material." Section 230(c) contains two distinct subsections that provide incentives for services to combat obscenity, "to help us control, at the portals of our computer, at the

front door of our house, what comes in and what our children see." *Id*.

Section 230(c) first provides that internet service providers who police obscenity will be in no worse position than providers who do nothing. Under Section 230(c)(1), "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." The sponsors suggested this text that, contrary to *Cubby*, expressly put providers that take measures to protect children from harmful content on the same plane as those who do not. It deems them distributors, rather than publishers or authors, of the content. Congress adopted this highly specific text. It easily could have made Section 230(c)(1) much broader by saying "interactive computer services shall not be held liable on account of information provided by another information content provider." It did not.

Section 230(c)(2) "responds . . . directly" to the decision in *Stratton*. *Force*, 934 F.3d 53 at 64 n.16. It provides incentives to internet service providers to "block[] and screen[] offensive material," by giving providers absolute immunity from anyone who might sue them for taking offensive content down or enabling others to block offensive content. 47 U.S.C. § 230(c)(2). This provision protects service providers from lawsuits by content providers whose content has been restricted. *See Enigma Software Grp. USA, LLC* v. *Malwarebytes, Inc.*, 946 F.3d 1040, 1046–47 (9th Cir. 2019) ("By immunizing internet-service providers from liability for any action taken to block, or help users block offensive and objectionable online content, Congress overruled *Stratton Oakmont* and thereby encouraged the development of more sophisticated

methods of online filtration."). Together, the two provisions in Section 230(c) ensure that a provider is not worse off by using its technology to keep obscenity out of the hands of children.

B. Factual Background.

1. Snapchat provides a robust environment for predators to groom and abuse minors. Its defining feature is that messages automatically disappear. Hillary Clinton famously joked about her e-mail issues on the campaign trail: "You may have seen that I recently launched a Snapchat account . . . I love it. Those messages disappear all by themselves." Erik Ortiz, *Hillary Clinton Has 'Love' for Snapchat in Joke About Email Scandal*, NBC News (Aug. 15, 2015), htt p: //tinyurl.com/5n6haczr. That joke had basis in reality—Snapchat is a place people go to engage in the most illicit behavior and remain undetected. That is what Snapchat is designed for.

Snapchat allows users to take photos and videos and send them to other users or post them to private groups or publicly. Jessica Glazer, *Snapchat's New Video Messages Feature Is Meant to Last Longer*, National Public Radio (May 4, 2014), http://tinyurl.com/ms866jyx. The photos and videos are ephemeral—they are only accessible for a short period of time and then they self-destruct. Jette Kofoed & Malene Charlotte Larsen, *A Snap of Intimacy: Photo-Sharing Practices Among Young People on Social Media*, First Monday, part 3 (Oct. 20, 2016), ht tp://tinyurl.com/6spv6u89 (Snapchat is "noteworthy and pioneering" because "content self-destructs after a short interval"). Individual messages are generally only available for seconds, or if set otherwise, for 24 hours. *Id*. "Stories," which are series of photographs

and/or videos posted to private groups or publicly, last 24 hours as a default. Darrell Etherington, *Snapchat Gets Its Own Timeline With Snapchat Stories, 24-Hour Photo & Video Tales*, TechCrunch (Oct. 3, 2013), http://tinyurl.com/2aajhhx5.

Shortly after Snapchat launched, it had a reputation as the place to send sexually explicit photos of oneself to other users. The Associated Press, *Snapchat CEO Evan Spiegel Talks Sexts and Growth*, The Denver Post (Nov. 10, 2013), http://tinyurl.com/422yunrz. Snapchat's value proposition was clear: young users "didn't want their social media history coming back to haunt them" later. O'Connell, *History of Snapchat*. From the beginning, Snapchat capitalized on a young user base. In a 2012 blog post, less than a year after launching, Snap's CEO gloated that leadership were "thrilled to hear that most of [Snapchat's users] were high school students who were using Snapchat as a new way to pass notes in class." Evan Spiegel, *Let's Chat*, Snapchat Blog (May 9, 2012), http://tinyurl.com/56hbmbx6. Snap is aware that most of Snapchat's users are young, and it *encourages* minors to lie about their ages by allowing users to change their ages up to five times. ER18.

Over time, Snapchat has added newer, more advanced opportunities for ephemeral messaging to and from children. February 2024 Investor Presentation at 10, Snap, Inc. (February 2024), http://tinyurl.com/3bfrnakc. That includes the ill-fated "SnapCash," which allowed peer-to-peer payments and was predictably used to sell sexually explicit photos. Christian Hargrave, *SnapCash Goes Away After Excessive Feature Misuse*, App Developer Magazine (July 25, 2018), http://tinyurl. com/3aaz2wka. That also includes Snapstreaks, which keep track of

consecutive usage days and rewards milestones. Avery Hartmans, *These Are the Sneaky Ways Apps Like Instagram, Facebook, Tinder Lure You in and Get You 'Addicted'*, Business Insider (Feb. 17, 2018), http: //tinyurl.com/nheyupsb ("Snapchat uses Snapstreaks to keep you hooked.") These features are designed to hook users, especially children, so they constantly engage. *Id*.

Knowing teen use drives revenue, Snapchat does not restrict the platform to adults. Anyone 13 years-old and up may join the platform. Sixty percent of U.S. teens aged 13–17 use Snapchat. Monica Anderson et al., *Teens, Social Media and Technology 2023*, Pew Research Center (Dec. 11, 2023), http: //tinyurl.com/4kehpc2f. Forty-three percent report being on Snapchat "almost constantly" or "several times a day." *Id*. And girls are more likely than boys to use Snapchat "almost constantly." *Id*. It is pervasive no matter the income level of the teenager's household. *Id*. Worse, as of 2021, 13% of children aged 8–12 were on Snapchat. Victoria Rideout et al., *The Common Sense Census: Media Use by Tweens and Teens, 2021*, Common Sense Media, 5 (2021), http://tinyurl.com/5n7v4xkx. Snap claims Snapchat does not allow users under 13, but it has admitted that Snapchat's existing age verification protocols on sign-up do not work. Isobel Asher Hamilton, *Snapchat Admits Its Age Verification Safeguards Are Effectively Useless*, Business Insider (Mar. 19, 2019), http://tinyurl. com/msber6tm.

With ephemeral messaging comes added danger. A study of American teens and pre-teens revealed that, among social media applications, Snapchat had "the highest number of survey participants reporting a potentially harmful online experience" at 26%.

Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking, Thorn 13 (May 2021), http://tinyurl.com/3kf7vzw3. It also—at 23% of the 9–17 year-olds studied—was "where the most participants said they have had an online sexual interaction." *Id.* And 15% of Snapchat users 9–17 reported having an online sexual interaction with someone they believed to be an adult. *Id.* at 15.

Unsurprisingly, many of these interactions are with predators. The self-destruction of messages makes Snapchat a haven for predators because it is "difficult for the police to collect evidence." Zak Doffman, *Snapchat Has Become a 'Haven for Child Abuse' With Its 'Self-Destructing Messages'*, Forbes (May 26, 2019), http://tinyurl.com/mr3hmuuy. One newspaper's investigation revealed "'thousands of reported cases that have involved Snapchat since 2014,' including 'pedophiles using the app to elicit indecent images from children and to groom teenagers.'" *Id.* A cybersecurity specialist has "warned parents that there is no safe way for kids to use the app as predators target children at random." Katie Davis, *"NO SAFE WAY TO USE IT" Snapchat is a "child predator's favorite app and parents shouldn't let their kids use it," cybersecurity expert warns*, The U.S. Sun (Aug. 6, 2021), http:// tinyurl.com/58bvcp6z.

2. Snapchat actively dupes parents into believing it has created a safe environment for their children. To assuage parents' fears, Snap represents Snapchat is a safe environment for its teen users. *Safeguards for Teens*, Snap, http://tinyurl.com/35cydvxt. Snap's Head of Global Platform Safety claims "[s]afety is part of the company's DNA" and under a section about "Strangers Finding Teens," she claims Snapchat "doesn't facilitate connections with unfamiliar people

like some social media platforms." Jacqueline Beauchere, *Meet Our Head of Global Platform Safety*, Snap, http://tinyurl.com/4m43axvz. Of course it does. In any event, she leaves out that it facilitates pornography, grooming, and other illicit behavior among familiar people. And Snap does little to nothing to stop child molesters. ER13.

Snap certainly *could* effectively combat human trafficking of minors. Snap boasts to advertisers that it can use Snapchat to target consumers by "location, demographics, interests, devices . . . and more!" ER18–19. And for advertisers, Snap moderates content to ensure that ads will not "show up next to something that could be harmful to your brand." ER19. Snap relies "heavily on [Snapchat's] ability to collect and disclose data, and metrics to our advertisers so we can attract new advertisers and retain existing advertisers." Snap Inc., Registration Statement (Form S-1) at 15 (Feb. 2, 2017), http:/ /tiny url.com/3zfw94v7. Notably, Snap does not purport to use any of these tools to prevent harm to teens on its page for parents. *Safeguards for Teens*.

Despite expressly adopting a duty to protect children from abuse, Snap only uses the data it mines to appease advertisers and thereby increase profits. ER13. "[I]t turns a blind eye and focuses only on tracking its users' activities in order to sell more ads." *Id*. This willful blindness, a design providing children unfettered access, and "Snapchat's disappearing-messages function provided the perfect cover and opportunity for [Plaintiff here, Doe's, teacher] to prey on her students." ER11.

3. When Doe was fifteen, his science teacher, who was in her thirties, groomed him, sexually assaulted

him, and induced his drug abuse. Pet. App. 4a. It was another miserable episode in a difficult childhood. When Doe was a child, his father abandoned him, and his mother was murdered. Pet. App. 5a. He had a legal guardian, but he also looked to school for a safe environment, where he trusted his teachers and the school staff. ER10.

Unfortunately, school was not a safe haven. Doe's teacher knew he was vulnerable and Snapchat was her way in. Pet. App. 6a. In October 2021, she asked Doe to stay after class, she closed the door, and she asked Doe for his Snapchat username. ER11. She then used Snapchat "to groom Doe by sending him sexually explicit content." Pet. App. 2a. Via Snapchat, she seduced him "by sending seductive photos of herself appended with solicitous messages." ER11. Snapchat's disappearing messages created a vital opportunity for the teacher to draw Doe in without leaving a trail. ER11. For over a year, the teacher continued this and ultimately began meeting him outside of class to engage in sexual conduct. Pet. App. 2a.

Having used Snapchat as her entry and to get Doe fully in her grasp, the teacher began to text Doe on his phone a couple of months into her sexual abuse. ER12. She got sloppy, telling him things like "don't forget the percs of th [sic] tutoring," with "percs" presumably meaning Percocet. ER12. Eventually, the abuse became known to other students. ER12. But Doe's guardian only discovered the teacher's behavior when Doe "overdosed on prescription drugs that were either provided or financed by" the teacher. Pet. App. 2a. Snap had all the tools to know a thirty-something woman was sending sexually explicit messages to a fifteen-year-old. ER19. Snap swore to

protect minors to get parents to let their children use its platform. ER19. And Snap did not use its resources to prevent Doe's sexual abuse. After all, if Snapchat limited what teenagers could consume, it might lose users—and consequently, advertising dollars.

C. Procedural Background.

1. Doe, through his guardian, Jane Roe, sued the teacher, the school district, and Snap. Pet. App. 6a–7a. Doe's claims against Snap are premised exclusively on Snap's conduct. His first cause of action against Snap is for negligent undertaking. ER18–20. Snap monitors users on Snapchat and mines content for all sorts of data to sell its services to advertisers. Yet it does *not* marshal those resources to protect children from predators Snap knows are drawn to its disappearing-messages service. "Having undertaken to monitor and profit from the data generated by user-created content, Snap, Inc. owes a duty under Texas law to perform that duty fully and reasonably." ER19. "Snap owes a duty to its minor users to protect them from sexual predators who are drawn to the Snapchat application by the privacy assurances granted by the disappearing messages feature of the application." *Id.*

Doe's second cause of action asserts negligent design. ER20. Snapchat is designed—with its defining feature being disappearing messages—to be used for illicit communication. *Id.* Yet Snap allows users as young as 13 years old to create an account and participate and its design functionally encourages children to lie about their ages. *Id.* "By creating an environment where adults can interact with underage users with assurances that there will be no long-

lasting evidence of those interactions, Snap has fostered an environment that draws in sexual predators and allows them to act with impunity." *Id.* Because of Snap's negligent design, Doe's teacher was able to seduce him, induce him to illegal drug abuse, and sexually assault him. *Id.*

In Doe's third and final cause of action, he asserts a claim for gross negligence. ER20–21. Rather than utilize the information it gathers to protect minors like Doe, Snap "made the conscious decision to use the information it gained only for its own financial gain." ER21. At the same time "it claims ignorance when minors are victimized in the same content it monitors." *Id.* Snap's conduct establishes conscious indifference to the severe risk of sexual molestation of minors that manifested here. *Id.*

Doe seeks to hold Snap liable for its own conduct in designing, managing, and promoting a service so that it would be used to abuse minors. Snap's offense was not publishing offensive materials; Doe wishes that was all he was exposed to. Snap created a place for child molesters to flourish and then drew minors in to be their victims, all the while proclaiming to parents and guardians that it would protect their children.

2. Snap moved to dismiss the complaint, asserting that 47 U.S.C. § 230 bars Doe's claims and any other claim that arises from a third party's use of Snapchat. Pet. App. 33a–34a. Citing Fifth Circuit precedent, the district court agreed with Snap that it was immune, stating that "'[n]o cause of action may be brought and no liability may be imposed under any State or local law' if the cause of action would 'make internet service providers liable for information originating with a

third-party user of the service.'" Pet. App. 34a (citations omitted). It thus adopted a standard whereby *anything* that involves third-party content triggers Section 230 immunity. The district court dismissed the complaint with prejudice as to Snap without allowing any amendment. Pet. App. 5a.

3. On appeal, the Fifth Circuit affirmed in an unpublished disposition. The panel stated it was bound by its 2008 decision, *Doe* v. *MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008), which held that Section 230 completely immunizes interactive computer services from claims involving third-party content. Pet. App. 3a.

The Fifth Circuit then *sua sponte* considered en banc review. Pet. App. 40a. Seven judges voted to review the case, eight judges voted against review, and two abstained. Pet. App. 41a. Judge Elrod filed a dissent from denial of rehearing en banc joined by the six other judges who voted in favor of rehearing. Pet. App. 41a.

Judge Elrod's dissent calls for the full circuit to "revisit[] our erroneous interpretation of Section 230" in *Doe* v. *MySpace*. Pet. App. 41a. It lays bare the errors in this precedent based on both text and policy. The dissent notes that Section 230(c)(1)'s statement that internet providers cannot be treated as "publishers or speakers" of third-party content does not reasonably mean that they are immune from *all* claims involving third-party content—including claims based on their own conduct, like design defect claims. Pet. App. 42a–43a. Holding otherwise, the dissent points out, creates a conflict with a related statute, which holds service providers liable "for knowingly displaying obscene material to minors"

regardless of whether the material was generated and directed to users by third parties. Pet. App. 43a (citing 47 U.S.C. § 223(d)).

The dissent further explains that "Congress used the statutory terms 'publisher' and 'speaker' against a legal background that recognized the separate category of 'distributors.'" Pet. App. 45a. (citing *Malwarebytes, Inc.* v. *Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 14 (2020) (Thomas, J., statement respecting denial of certiorari)). Because distributors are only liable for content for which they had or should have had knowledge, Section 230(c)(1) simply displaces strict liability for content as publishers. Pet. App. 45a. It does not displace distributor liability and it certainly does not displace general liability for design defects. Pet. App. 45a.

Finally, the dissent explains that with the internet's exponential growth, service providers "monitor and monetize content, while simultaneously promising to protect young and vulnerable users." Pet. App. 46a. Service providers are "no longer the big bulletin boards of the past;" rather, "they are complex operations offering highly curated content." Pet. App. 47a. As such, today's internet service providers cannot reasonably enjoy unchecked immunity when they exercise great power over information and content. Pet. App. 47a.

REASONS FOR GRANTING THE WRIT

I. The question presented requires this Court's review.

A. The Court already recognized the need to review the scope of Section 230, granting certiorari in *Gonzalez* v. *Google*.

In October of 2022—approximately 16 months ago—this Court "granted certiorari" in *Gonzalez* v. *Google* "to review the Ninth Circuit's application of § 230." *Gonzalez* v. *Google LLC*, 598 U.S. 617, 622 (2023). At the time it granted the *Gonzalez* petition, this Court, indisputably, acknowledged the need to review the circuit courts' interpretations of Section 230. *Id.* In the years prior, Justice Thomas had repeatedly urged the Court to "address the proper scope of immunity under § 230 in an appropriate case." *Doe* v. *Facebook, Inc.*, 142 S. Ct. 1087, 1088–89 (2022) (Thomas, J. respecting the denial of certiorari) (noting the case was not appropriate because it was still ongoing, meaning the court lacked jurisdiction because there was not yet a "[f]inal judgement[] or decree[]" to review); *Malwarebytes, Inc.* v. *Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 18 (2020) (Thomas, J. respecting the denial of certiorari) ("[W]e need not decide today the correct interpretation of § 230. But in an appropriate case, it behooves us to do so.").

Unfortunately, *Gonzalez* was not the appropriate case. The Court was unable to answer the question presented because of a latent defect. The Court "decline[d] to address the application of § 230" to plaintiffs' complaint because, in light of its decision in *Twitter, Inc.* v. *Taamneh*, 598 U.S. 471 (2023), it

appeared plaintiffs' complaint failed to state a "plausible claim for relief." 598 U.S. at 622. Plaintiffs' claims were "materially identical to those at issue in" *Twitter*. *Id*. So when the Court determined the plaintiff in *Twitter* failed to state a viable claim for relief, it concluded the plaintiff in *Gonzalez* likely did too. The Court remanded the case without taking up Section 230, thus leaving this pressing question unanswered.

B. The circuits are lost on how to interpret Section 230.

The lower courts are divided over the proper application of Section 230(c)(1). The divide is lopsided, with nearly all of the circuits, save the Seventh, mistakenly following the lead of one early case. That case announced that Section 230(c)(1) grants internet service providers "broad immunity" for almost all conduct involving third-party content, regardless of the role the platform played and the claim asserted. In recent years a growing chorus of judges from these circuits have spoken out, declaring the leading interpretation of Section 230(c)(1) was wrong from the start and even more problematic in light of the proliferation and sophistication of the public's internet use today. Now ten circuit judges have called for this Court's intervention on this issue.

1. From the earliest cases, the lower courts mistakenly applied Section 230(c)(1). "[T]he first appellate court to" address Section 230(c)(1)'s scope was the Fourth Circuit in *Zeran* v. *Am. Online, Inc.*, 129 F.3d 327 (4th Cir. 1997). *See Malwarebytes*, 141 S. Ct. at 15. The complaint alleged AOL committed various torts when it "unreasonably delayed . . . removing defamatory messages" about the plaintiff

that an unknown user had posted to AOL's online "bulletin boards," "refused to post retractions of those messages, and failed to screen for similar postings thereafter." *Zeran*, 129 F.3d at 328–29.

Affirming judgment on the pleadings, the Fourth Circuit found AOL immune from all of the plaintiff's claims under Section 230(c)(1) in a sweeping opinion. *Id*. at 330. Focusing on the "policy" and "purpose" behind the statute, the Fourth Circuit concluded "§ 230 creates a federal immunity [for] *any* cause of action that would make service providers liable for information originating with a third-party user of the service." *Id*. (emphasis added). Because all the plaintiff's claims centered on the unknown poster's defamatory statements, the Fourth Circuit found AOL entirely immune from suit. *Id*.

The Fourth Circuit did not stop there. It also squarely rejected the plaintiff's argument that Section 230 "eliminates only publisher liability," but leaves "distributor liability intact." *Id.* at 331. As the plaintiff correctly pointed out, Section 230(c)(1) says that no "interactive computer service shall be treated as the *publisher* or *speaker* of any information provided by another information content provider," (emphasis added) but says nothing about whether it may be treated as a "distributor" of such content, nor does it state providers shall be "immune." *Id.* at 330–331. Nevertheless, the Fourth Circuit concluded the plaintiff read too much "significance" into the legal distinction between publisher and distributor and that "distributor liability . . . is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230." *Id.* at 332. In other words, the Fourth Circuit did the exact opposite of what the sponsors of Section 230 intended: It took the decision

in *Cubby* that Section 230's sponsor decried and *expanded* its protection for internet platforms that do nothing to protect users.

2. This abject failure to follow both text and purpose caught on. Following *Zeran*'s lead, "[t]he majority of federal circuits" have interpreted Section 230(c)(1) "to establish broad 'federal immunity . . . '" for online platforms from "*any* cause of action" involving third-party created content.[2] *See Almeida* v. *Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006) (emphasis added) (quoting *Zeran*); *see also MySpace*, 528 F.3d at 418 (agreeing with other "[c]ourts [that] have construed the immunity provisions in § 230 broadly in all cases arising from the publication of user-generated content") (citing, inter alia, *Zeran*); *Jones* v. *Dirty World Ent. Recordings LLC*, 755 F.3d 398, 406–07 (6th Cir. 2014) ("Although § 230(c)(1) does not explicitly mention immunity or a synonym thereof, this and other circuits have recognized the provision" "immunizes providers of interactive computer services against liability arising from content created by third parties.") (citing, inter

---

[2] Several state Supreme Courts, relying on *Zeran*, have similarly concluded that Section 230(c)(1) "afford[s] interactive service providers broad immunity from tort liability for third party speech." *Hassell* v. *Bird*, 5 Cal. 5th 522, 420 P.3d 776, 782, 785 (2018); *Doe* v. *Am. Online, Inc.*, 783 So. 2d 1010, 1013–17 (Fla. 2001) ("We find persuasive the reasoning of . . . the Fourth Circuit in *Zeran*[.]"); *Shiamili* v. *Real Est. Grp. of New York, Inc.*, 17 N.Y.3d 281, 288, 952 N.E.2d 1011 (2011) ("Both state and federal courts around the country have 'generally interpreted Section 230 immunity broadly[.]'") (quoting extensively from *Zeran*); *Daniel* v. *Armslist, LLC*, 2019 WI 47, 386 Wis. 2d 449, 464, 926 N.W.2d 710, 717 ("Section 230(c)(1) . . . immuniz[es] interactive computer service providers from liability for publishing third-party content.").

alia, *Zeran*); *Marshall's Locksmith Service Inc.* v. *Google, LLC*, 925 F.3d 1263, 1267 (D.C. Cir. 2019) ("§ 230 immunizes internet services for third-party content that they publish . . . against causes of actions of all kinds.").

The Seventh Circuit is the lone outlier in sticking to Section 230's text and declining to follow *Zeran*'s lead. It has repeatedly recognized that Section 230(c)(1) does not create immunity at all. *Doe* v. *GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003) (Section 230(c)(1) is "a definitional clause rather than . . . an immunity from liability"). In the Seventh Circuit's view "§ 230(c)(1) forecloses any liability that depends on deeming the ISP a 'publisher'—defamation law would be a good example of such liability—while permitting the states to regulate ISPs in their capacity as intermediaries." *Id.*; *see also City of Chicago, Ill.* v. *StubHub!, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010). As one Seventh Circuit panel aptly explained, other circuits' broad interpretation of Section 230 would also immunize websites like Napster "designed to help people steal music" or other material protected by copyright, a position "incompatible" with this Court's opinion in *Metro–Goldwyn–Mayer Studios Inc.* v. *Grokster, Ltd.*, 545 U.S. 913 (2005). *Chicago Lawyers' Comm. for C.R. Under L., Inc.* v. *Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008).

As the years passed, and social media and internet use proliferated—and became more sophisticated—courts applied the "broad immunity" announced in *Zeran* and to various claims. Courts have found Section 230(c)(1) immunizes online platforms from claims that the design and features of their websites facilitate human trafficking and child sex trafficking.

Jane Doe No. 1 v. *Backpage.com, LLC*, 817 F.3d 12, 16–21 (1st Cir. 2016); *M.A. ex rel. P.K.* v. *Vill. Voice Media Holdings, LLC*, 809 F. Supp. 2d 1041, 1048–49 (E.D. Mo. 2011). Other courts immunized social media platforms from claims that their recommendation algorithms promote and contribute to terrorist activity. *See Force* v. *Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019) (finding Facebook immune from federal anti-terrorism claims that its algorithms enabled Hamas terrorist attacks in Israel); *Gonzalez* v. *Google LLC*, 598 U.S. 617 (2023) (finding numerous social media platforms immune from anti-terrorism claims that their recommendation algorithms promoted and furthered ISIS terrorist attacks). Still others have found Section 230(c)(1) immunizes app developers for failing to include safety features to protect users from impersonation, harassment, and "other dangerous conduct" performed by other app users. *See Herrick* v. *Grindr LLC*, 765 F. App'x 586 (2d Cir. 2019) (app developer immune from claims that its "'hook-up' application" was defectively designed because it permitted third-party to impersonate plaintiff and direct other users to plaintiff's home).

3. The ever-expanding scope of "Section 230(c)(1) immunity" outside the Seventh Circuit has drawn skepticism from some and vigorous dissents from others. In *Force*, Second Circuit Chief Judge Katzmann pushed back against the majority's further extension of this questionable precedent. Judge Katzmann dug deep into the text and legislative history of Section 230 to conclude the statute "does not protect Facebook's friend- and content-suggestion algorithms." 934 F.3d at 82. As Judge Katzmann explained, Facebook cannot be immune from claims arising from *its own* messaging and *its own* conduct,

both of which fall far outside the scope of Section 230(c)(1) protection. *Id.* at 77–84 (criticizing majority for "extend[ing] 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").

In *Gonzalez*, Ninth Circuit Judges Berzon and Gould "join[ed] the growing chorus of voices calling for a more limited reading of the scope of section 230 immunity." *Gonzalez* v. *Google LLC*, 2 F.4th 871, 913–52 (9th Cir. 2021). Judge Berzon concurred but wrote that "if not bound by Circuit precedent, [she] would hold that" Section 230(c)(1) does not protect "activities that promote or recommend content or connect content users to each other" like the recommendation algorithms utilized by social media platforms. *Id.* at 913. Like Judge Katzmann, Judge Berzon explained "the term 'publisher' under section 230 reaches only traditional activities of publication and distribution—such as deciding whether to publish, withdraw, or alter content." *Id.* "Nothing in the history of section 230 supports a reading of the statute so expansive as to" include "targeted recommendations and affirmative promotion of connections and interactions among otherwise independent users" as "traditional" publisher functions. *Id.* at 914–15.

Judge Gould went farther. He dissented from the majority's immunity findings, attaching the entirety of "Chief Judge Katzmann's cogent and well-reasoned opinion . . . in *Force*" to his dissent. *Id.* at 920, 938–52. In Judge Gould's "view, Section 230 was not intended to immunize," and should not be read to "give social media platforms total immunity" for all

claims involving user-generated content. *Id.* at 920, 921. Judge Gould would have held "that Plaintiffs' claims do not fall within the ambit of Section 230 because Plaintiffs d[id] not seek to treat Google as a publisher or speaker of the ISIS video propaganda." *Id.* at 921.

Finally, in this case *seven* judges from the Fifth Circuit, led by Judge Elrod, joined the chorus calling for change. The district court and the Fifth Circuit panel followed settled Fifth Circuit precedent in finding Snap immune from suit under Section 230. The judges in dissent from denial of en banc rehearing voted to "revisit[]" the Fifth Circuit's "erroneous interpretation of Section 230" that granted "sweeping immunity for social media companies." Pet. App. 41a. As these judges recognize, Doe seeks to hold Snap liable for its "own conduct" in defectively designing its application and for knowingly distributing harmful content. Pet. App. 44a. "Nowhere in its text does Section 230 provide immunity" from such claims, Judge Elrod explained, yet under the Fifth Circuit's "overbroad reading of Section 230," Plaintiff's claims were deemed "dead in the water." Pet. App. 44a–45a.

The call of these ten circuit judges is clear. Only this Court's intervention can end the abusive, atextual immunity that divides the circuits once and for all.

C. This case presents a question of exceptional importance.

Section 230's scope is a critical legal issue that is repeatedly, and increasingly, litigated in the lower courts. *See Malwarebytes*, 141 S. Ct. at 14 (describing Section 230 as an "increasingly important statute"). But this case, which highlights the dangers of social

media use for children, brings the importance of this issue into even sharper focus. Social media use, especially among American teens, is rampant. Social media platforms, like Snapchat, have created dangerous online environments where children are easy targets for exploitation and abuse. Meanwhile, courts have interpreted Section 230 "to confer sweeping immunity" on social media companies, *Malwarebytes*, 141 S. Ct. at 13, removing all incentives for them take any steps to protect children and removing all avenues to hold them accountable for their own misconduct. In addition, as was the case here, most claims alleging serious wrongdoing by internet platforms are dismissed under Section 230 at the pleading stage, before plaintiffs ever have an opportunity to develop any evidence to reveal the true nature and extent of these companies' misconduct. In short, the magnitude of this issue demands this Court's immediate intervention.

The question presented impacts the vast majority of youth in this county. "Smartphone ownership is nearly universal among teens," with no differences amongst "genders, ages, races and ethnicities, [or] economic backgrounds." Anderson, *Teens, Social Media and Technology 2023*. Teens use smartphones relentlessly. The average American teenager's screen time is 7 hours a day, excluding homework time. *See* Jay N. Giedd, *Adolescent Brain and the Natural Allure of Digital Media*, 22 DIALOGUES IN CLINICAL NEUROSCIENCE, 127 (2020). Social media is the primary driver of this use. "Up to 95% of youth ages 13–17 report using a social media platform, with more than a third saying they use social media 'almost constantly.'" *Social Media and Youth Mental Health:*

the U.S. Surgeon General's Advisory, U.S. Dep't Health & Hum. Servs. (May 23, 2023) at 4.

Minor abuse on social media platforms is widespread and has increased dramatically in recent years. In 2022 alone, the National Center for Missing & Exploited Children ("NCMEC") received over 32 million reports of suspected online child exploitation. *CyberTipline 2022 Report*, NCMEC, http://tinyurl.com/2vsd6pps. That number includes over 80,000 reported instances of "Online Enticement of Children for Sexual Acts," an 82% increase from the year before, and over 35,000 reported instances of "Unsolicited Obscene Material Sent to a Child," a sevenfold increase from the year before. *Id.*

There is little mystery behind this troubling expansion of online child abuse. The same design features that Snap and other platforms employ to drive teenage engagement turn into weapons in the hands of predators. Where minors create multiple social media accounts without background, age, or identity checks (as is commonly the case with "finstas" ("fake Instagrams")), predators similarly create various profiles under different pseudonyms to target different victims. Where minors receive recommendations for and join various social media groups to develop their interests and find communities they belong in, predators use these affiliations to begin establishing themselves as trust figures to potential victims. Where minors use social media platforms' instant messaging functions to stay connected with friends near and far, predators use those functions to constantly contact and coerce potential victims from any distance, at volume. Where minors use social media to update their networks on their lives, predators extract personally

identifiable information from potential victims' accounts to further encroach upon their lives.

With Section 230 immunity in hand, social media platforms are doing next to nothing to address the dangers their platforms pose to children for fear that any action they take might also decrease membership, usage, and revenue. For example, Snapchat's latest transparency report states that its process for detecting child sexual abuse on its platform consists of "identify[ing] *known* illegal images and videos of child sexual abuse" and reporting them "as required by law." *Transparency Report: January 1, 2023 – June 30, 2023*, Snap, http://tinyurl.com/43fmwbru. But Snapchat's primary purpose is to facilitate the sharing of *new, real-time* photos and videos. Apparently, Snap has no process for detecting or reporting child sexual abuse material generated on its own platform. As another example, an internal study leaked by a whistleblower reported that 13% of all Instagram users aged 13 to 15 received unwanted sexual advances over just seven days. *Social Media and the Teen Mental Health Crisis*: *Before the Subcomm. On Privacy, Technology, and the Law of the H. Comm. On the Judiciary*, 118th Cong. 4 (2024) (written testimony of Arturo Bejar). Despite having clear confirmation of this consistent abuse, Meta—Instagram's owner—has done nothing to protect these vulnerable users.

The import of the question presented is clear. Social media companies must be held accountable for the harms they are imposing on America's youth through their own misconduct. But only this Court can remove the atextual immunity that lower courts have read into Section 230 to protect them.

II. This case presents the ideal vehicle for resolving the question presented.

This case presents the strongest vehicle yet to resolve the meaning of Section 230(c)(1).

1. This case is the ideal vehicle because it cleanly raises the question presented. Both the district court's and the Fifth Circuit's decisions below turned entirely on Snap's asserted immunity from suit under Section 230 and cited no alternative grounds for their decisions. The district court dismissed all of Doe's claims—negligent undertaking, negligent design, and gross negligence—based on Section 230 immunity, and the Fifth Circuit squarely and succinctly affirmed. Finally, the Fifth Circuit rejected the call for en banc review. In short, this entire case turns on Section 230 and all avenues of lower court review have been exhausted.

This case also addresses two underlying questions regarding the scope of Section 230 that have confounded lower courts. First, Doe's negligent undertaking claim raises the question of whether Snap can be held liable as a distributor of harmful content, rather than a publisher, under Section 230. This claim asserts Snap knew, or should have known, of the illicit nature of the communications between Doe and his teacher on its platform. If this Court finds Section 230 does not immunize distributor liability, Doe can proceed with his negligent undertaking claim against Snap. Second, Doe's design defect claim raises the question of whether Section 230 prevents Snap from being held liable for conduct that falls outside of the publisher/distributor dichotomy. The design defect claim seeks to hold Snap liable for its design choices that knowingly invite children into a

lair of pedophiles and protect their abuses once they get there. If this Court finds Section 230 does not immunize a platform's own misconduct, Doe can proceed with his design defect claim against Snap.

Finally, this case presents the perfect prism through which to view Section 230 because it implicates the particular evil of the internet—child sexual abuse, pornography, and obscenity—that Section 230 was specifically enacted to *prevent*. Congress's clear intent in passing Section 230 was to protect children from sexual dangers on the internet and Section 230(c) in particular was designed to encourage providers like Snapchat to protect children. *See infra* pp. 5–8. It was not enacted to provide cover for the abject failure to protect children while also designing a haven for pedophiles. Through this case, the Court can directly evaluate whether the Fifth Circuit's approach to Section 230 aligns with the text and original intent of the statute.

2. Broad immunity under Section 230 should be resolved here. For years, social media companies have assured this Court that Congress is right in the midst of working on it. *See, e.g.*, Brief in Opposition, *Gonzalez* v. *Google LLC*, No. 21-1333, at 18–20; Brief in Opposition, *Force* v. *Facebook, Inc.*, No. 19-859 at 29–30. Snap may repeat this overture, pointing to the dozen or so pieces of draft legislation currently pending in Congress proposing to alter Section 230. *See All the Ways Congress Wants to Change Section 230*, Slate (updated Sept. 19, 2023), http://tinyurl.com/47vamwwr. Snap may also point to the recent U.S. Senate Judiciary Committee hearings to examine protecting kids online—at which it testified—as evidence that Congress is finally getting serious about addressing this issue. *Big Tech and the Online Child*

Sexual Exploitation Crisis: Hearing Before the S. Comm. On the Judiciary, 118th Cong. (Jan. 31, 2024).

Congress has had more than 25 years to clarify Section 230(c)(1) in response to incorrect judicial interpretations. It has not done so and it almost certainly will not do so now. None of the currently pending legislation carries any certainty of passing, of bringing the change needed to hold social media platforms responsible for the abuse that occurs on and with the assistance of their platforms, or of helping those like Doe who have already been harmed. Moreover, Congress has held similar hearings in the past and afterward done nothing to address Section 230. *See, e.g., Protecting Kids Online: Snapchat, TikTok, and YouTube, Hearing Before the S. Subcomm on Consumer Protection, Product Safety, & Data Security*, 117th Cong. (Oct. 26, 2021). Even if there were any hope of Congressional action, this Court should not sit on its hands waiting for Congress to do something when, properly interpreted, Section 230 does not bar claims, like Doe's, which are based on an internet platform's own misconduct. Overbroad immunity under Section 230 is a judicially created problem, and this Court's intervention is the solution.

CONCLUSION

For the foregoing reasons, the petition should be granted, the judgment below should be reversed, and the case should be remanded for further proceedings.

Respectfully submitted,

PETER K. STRIS
STRIS & MAHER LLP
777 S. Figueroa Street, Suite 3850
Los Angeles, CA 90017

DEREK MERMAN
HEARD MERMAN LAW FIRM
4900 Fournace Place, Suite 240
Bellaire, Texas 77401

TILLMAN J. BRECKENRIDGE
COUNSEL OF RECORD
COLLEEN R. SMITH
STRIS & MAHER LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 800-6030
tbreckenridge@stris.com