No. 24-475

In the United States Court of Appeals for the Ninth Circuit

JOHN DOE, an individual,

Plaintiff-Appellant,

v.

GRINDR INC.; GRINDR LLC,

Defendants-Appellees.

On Appeal from the United States District Court
for the Central District of California, Los Angeles
Case No. 2:23-cv-02093-ODW-PD (The Hon. Otis D. Wright)

BRIEF OF AMERICAN ASSOCIATION FOR JUSTICE AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT

JEFFREY R. WHITE
Senior Associate General Counsel
AMERICAN ASSOCIATION FOR JUSTICE
777 6th Street NW, #200
Washington, DC 20001
(202) 617-5620

MATTHEW W.H. WESSLER
ALISA TIWARI
GUPTA WESSLER LLP
2001 K Street NW, Suite 850 North
Washington, DC 20006
(202) 888-1741
matt@guptawessler.com

May 17, 2024

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* the American Association for Justice states it is a non-profit organization. It has no parent corporation or publicly owned corporation that owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The American Association for Justice is a national, voluntary bar association established in 1946 to strengthen the civil justice system, preserve the right to trial by jury, and protect access to the courts for those who have been wrongfully injured. With members in the United States, Canada, and abroad, AAJ is the world's largest plaintiff trial bar. AAJ members primarily represent plaintiffs in personal injury actions, employment rights cases, consumer cases, and other civil actions, including product liability actions against social media applications. Throughout its 77-year history, AAJ has served as a leading advocate for the right of all Americans to seek legal recourse for wrongful conduct.

[1] All parties consent to the filing of this brief, and no counsel for any party authored it in whole or in part. Apart from the amicus curiae, no person, party, or party's counsel contributed money intended to fund the brief's preparation and submission.

INTRODUCTION & SUMMARY OF ARGUMENT

The complaint in this case alleges that Grindr matches children with adults for sex. If a brick-and-mortar matchmaker did that, there would be no dispute that its conduct was illegal. Yet Grindr claims that because it operates over the internet, Section 230 immunizes it for this conduct. That's wrong. This Court has "consistently eschewed an expansive reading of the statute that would render unlawful conduct magically . . . lawful when [conducted] online, and therefore giv[ing] online businesses an unfair advantage over their real-world counterparts." *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 683 (9th Cir. 2019).

The reason for that is simple. Section 230 does not immunize a company's *own* unlawful conduct. Rather, it only protects companies from being held liable for "publication"—that is, for "reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1091 (9th Cir. 2021) (quoting *HomeAway.com*, 918 F.3d at 618). In practice, that means a plaintiff's claim must be based on the company's dissemination of "improper" third-party content. *Henderson v. Source for Pub. Data, L.P.*, 53 F.4th 110, 122 (4th Cir. 2022). Or, as this Court has put it, the duty underlying the plaintiff's claims must leave the company no choice but to "edit[], monitor[], or remov[e]" content posted by a company's users. *Lemmon*, 995 F.3d at 1092. Thus, claims that Twitter or Facebook disseminated illegal content (*e.g.*, defamatory or discriminatory posts) are barred. *See*

id. at 1091–92. But claims that those companies themselves designed a defective product are not. *See id.*

So, how does that work here? Start with the facts. Grindr is essentially an online match-making service for sex. Users sign up, create dating profiles, and send their geolocations to the company so it can match them to the closest one hundred other users. Matched users can then connect using private messages to arrange an in-person sexual encounter. On paper, everyone agrees that only adults should be using Grindr. For good reason: sexual encounters between children and adults are illegal. Yet Grindr designed its app so children can easily use it: Grindr has no age verifications at registration, and it indiscriminately matches anyone using the app based on geolocation. And so children do use it and are raped, as lawsuits and news articles have made clear. But instead of warning children of this known risk, Grindr *encourages* them to sign up on TikTok and Instagram. Doe suffered the consequences of Grindr's actions, and he now seeks to hold the company liable.

Section 230 shouldn't provide a shield for Grindr's actions. Doe's product liability claims, for instance, that Grindr designed an unreasonably dangerous app implicates Grindr's own design choices—not the company's dissemination of improper third-party content. And the negligent misrepresentation and failure-to-warn claims also implicate Grindr's own conduct. The former seeks to hold Grindr accountable for its own misrepresentations, while the latter for its own failure to alert

children to an obvious danger. Because these claims have "nothing to do with its editing, monitoring, or removing of the [profile and messaging] content that its users generate through [Grindr]," Section 230 should not provide immunity from suit. *Lemmon*, 995 F.3d at 1092.

ARGUMENT

I. Congress enacted Section 230 to ensure that internet companies do not face liability for publishing the words of others.

Section 230 was passed in the mid-nineties, when the internet was, to most people, "an absolutely brand-new technology." 141 Cong. Rec. 8469 (1995) (statement of Rep. Christopher Cox). But public access to the internet was growing. *See* Susannah Fox & Lee Rainie, Pew Rsch. Ctr., *The Web at 25 in the U.S.* (Feb. 27, 2014), https://perma.cc/9Q5L-DCMU. And while there was much excitement about the potential of this new technology, the public—and Congress—had one major concern: "smut," and particularly the extent to which the internet would make it available to children. *See, e.g.*, 141 Cong. Rec. 8470 (1995).[2]

In 1995, a study demonstrating the ubiquity of pornography on the internet—and expressing concern that there was no way to prevent children from accessing it—received widespread press attention. *See* Marty Rimm, *Marketing Pornography on the Information Superhighway*, 83 Geo. L.J. 1849, 1858 (1995). The study spawned

[2] Unless otherwise specified, all internal quotation marks, citations, emphases, and alterations are omitted from quotations throughout this brief.

"endless articles and editorials." Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 Fed. Commc'ns L.J. 51, 53–54 (1996). The July 1995 cover of Time Magazine screamed "CYBERPORN" in all caps, over an image of a wide-eyed toddler sitting at a keyboard. *Cyber Porn*, TIME (July 3, 1995), https://perma.cc/Q23P-T6SC. And within days, the Time article was reprinted in the Congressional Record and cited by senators railing against the "flood of vile pornography" in cyberspace. 141 Cong. Rec. 17083 (1995).

In both the House and the Senate, legislator after legislator rose to speak about the need to protect children from internet porn. *See, e.g.*, 141 Cong. Rec. 8469–8472 (1995); 141 Cong. Rec. 17083 (1995); 141 Cong. Rec. 8293, 8329–48 (1995). Both chambers sought to deal with the issue through amendments to the Telecommunications Act of 1996—a statute that otherwise had little to do with the internet, but instead was aimed at overhauling the regulations governing the telephone and cable industries "to promote competition." *See Reno v. Am. C.L. Union*, 521 U.S. 844, 857 (1997). While most of the Telecommunications Act was thoroughly examined and debated—"the product of extensive committee hearings" and multiple reports—the amendments targeted at internet pornography were little considered, added on as an afterthought. *Id.* at 858.

The two chambers took vastly different approaches to the problem. The Senate passed the Exon Amendment, which criminalized making "indecent" material available to minors. *See* 141 Cong. Rec. 8386 (1995). The House, however, believed that prohibiting indecent content would not solve the problem. House members expressed concern that such an approach would be both expensive and ineffective—a costly game of whack-a-mole that, given the breadth of the internet, the government could never win. *See, e.g.*, 141 Cong. Rec. 8469–72 (1995). And, they feared, the criminalization of content based on vaguely defined terms like "indecent" could amount to broad government censorship. *See id.* at 8470.

As the co-sponsor of the House amendment put it: The Senate's approach would "essentially involve the Federal Government spending vast sums of money trying to define elusive terms that are going to lead to a flood of legal challenges while our kids are unprotected." *Id.* (statement of Rep. Ron Wyden). "The fact of the matter," he explained, "is that the Internet operates worldwide, and not even a Federal Internet censorship army would give our Government the power to keep offensive material out of the hands of children who use the new interactive media." *Id.*; *see also id.* ("[I]f there is this kind of Federal Internet censorship army that somehow the other body seems to favor, it is going to make the Keystone Cops look like crackerjack crime-fighter.").

The House, therefore, sought to empower internet companies, like websites and internet service providers, to themselves filter out offensive content—and build tools for parents (and other internet users) to do the same. *See* 141 Cong. Rec. 8469–72 (1995). The problem, as the House saw it, was the existing legal regime, under which internet companies that filtered the content posted by their users risked being held liable for that content, whereas companies that allowed users to post anything they wished bore no such risk. *See, e.g.*, *id*.

In particular, the House focused on a recent New York state court decision, which relied on a longstanding rule of defamation law that distinguished between distributors and publishers. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995). Distributors, such as bookstores or magazine stands, the court explained, are entirely passive conduits for information; and so, they are only liable for defamation if they know the content they're selling is defamatory. *See id.* Publishers, on the other hand—newspapers or magazines, for example—are not passive; they make choices about what content gets published. *See id.* They are, therefore, equally "subject to liability" for defamation as the person who made the defamatory statement in the first place. *See id.*

As applied to the internet, *Stratton Oakmont* held that an internet company that allows users to post anything they wish, without exercising any control over what is or isn't published, is a mere distributor. *See id.* But a website that reviews user posts

and takes down offensive content, the court concluded, is no different than a newspaper or magazine—a publisher subject to precisely the same liability for defamatory content as the user who posted it. *See id.*

This rule, House members believed, was "backward." 141 Cong. Rec. 8470 (1995). The law, in their view, should "encourage" internet companies to screen out offensive content posted by their users, not punish them for it. *Id.* And so the House sought to remedy the problem by passing an amendment that would reverse the *Stratton Oakmont* decision—and prohibit websites and internet service providers from being held liable for content posted by their users simply because they chose to remove some of that content. *See id.*

Surprisingly, the final statute contained versions of both the House and Senate amendments. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 561(b), 110 Stat. 56, 143. The Senate amendment was swiftly struck down by the Supreme Court as vague and overbroad in violation of the First Amendment. *Reno*, 521 U.S. at 859–60, 885. But the House amendment survived as what's now known as Section 230.

The House's goal—ensuring that internet companies don't face liability for policing content posted by their users—is evident throughout the Section. The title of Section 230 as a whole is "Protection for private blocking and screening of offensive material." 47 U.S.C. § 230. And the title of its operative provision, Section 230(c), is "Protection for 'Good Samaritan' blocking and screening of offensive

material." *Id.* § 230(c). Section 230(c) protects internet companies' ability to screen their users' content in two ways. First, it states that "[n]o 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." *Id.* § 230(c)(1). And second, it ensures that "[n]o provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to" material they believe is "objectionable" or enable others to do so. *Id.* §§ 230(c)(2), 230(c)(2)(A). In other words, the law prohibits internet companies from being held responsible for content posted by someone else—even when they remove or restrict access to some of that content.

The conference report on the Telecommunications Act confirms the purpose of these provisions that is evident from their text and the debate leading up to their passage: to "overrule *Stratton Oakmont* and any other similar decisions" and to provide "protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material." S. Rep. No. 104-230, at 194 (1996) (Conf. Rep.). Nothing in the text of the statute or its legislative history indicates that Congress sought to immunize internet companies for conduct that has nothing to do with the publication of someone else's speech.

II. Section 230 only provides internet companies with immunity from liability for the content of information posted by someone else.

1. Section 230(c)(1) 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." Thus, Section 230 shields internet companies from claims that "treat[]" them "as the publisher . . . of [] information provided by" someone else.[3]

Although Section 230 does not define the term "publisher," its ordinary meaning is well-established. A publisher is one who "disseminate[s]" work to the public. Publish, *Merriam-Webster's Collegiate Dictionary* 944 (1994); *see* Publisher, *Webster's Third New International Dictionary* 1837 (Philip Babcock Gove ed. 1986). A publisher thus "review[s], edit[s], and decid[es] whether to publish or to withdraw from publication third-party content." *Lemmon*, 995 F.3d at 1091. As this Court has repeatedly explained, to "treat" an internet company as a "publisher[]," therefore, is to impose liability on that company for "exercis[ing]" these "traditional editorial functions"—that is, to hold the company liable for third-party content. *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1184–85 (9th Cir. 2008); *accord, e.g.*, *HomeAway.com, Inc. v.*

[3] There are additional requirements for Section 230 immunity that may be relevant here. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1091 (9th Cir. 2021) (explaining that, for immunity, a defendant must be "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider"). This brief, however, only addresses the "publisher" requirement.

City of Santa Monica, 918 F.3d 676, 681 (9th Cir. 2019) (no immunity because the defendants "face[d] no liability for the content of [third-party posts]").

This concept of "publisher" liability did not originate with Section 230; it has deep roots in the common law. *Henderson v. Source for Pub. Data, L.P.*, 53 F.4th 110, 122 (4th Cir. 2022) (tracing history). "[T]o hold someone liable as a publisher at common law was to hold them responsible for" disseminating content of an "improper nature." *Id.* Defamation is the paradigmatic example: Holding the New York Times liable for publishing an article that falsely claims its subject is a murderer imposes "publisher" liability on the newspaper. *See id.* "Other information-based torts at common law follow this mold, imposing liability on publishers for the improper nature of their disseminated content." *Id.* at 122 n.15. Thus, when Congress mandated that internet companies not be "treated" as the "publisher" of content posted by their users, it was mandating that courts not impose liability on them for disseminating "improper" third-party content. *Id.* at 122 & n.11; *see HomeAway.com*, 918 F.3d at 682.

This Court has held that to determine whether a plaintiff's claims run afoul of this requirement, "we focus on . . . the duty the plaintiff" seeks to impose on the defendant. *Lemmon*, 995 F.3d at 1091. If the duty underlying the plaintiff's claims is a duty to "edit[], monitor[], or remov[e]" content posted by a company's users, the claims seek to impose "publisher" liability—and are barred by Section 230. *Id.* That makes sense: If a company must review or filter information that users post to satisfy a legal duty, then the plaintiff is

seeking to hold the company liable for the existence of certain content. But where a plaintiff's claims impose no such duty, Section 230 does not apply. *Id.*; *accord HomeAway.com*, 918 F.3d at 682.

This Court explained the distinction between publishing and non-publishing duties in *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009). There, the plaintiff sued Yahoo for failing to remove indecent profiles of her that her ex-boyfriend had made. *Id.* at 1098–99. This Court held that Section 230 immunized Yahoo from claims that it was negligent for failing to remove the profiles, because "removing content is something publishers do." *Id.* at 1103. But the plaintiff also brought a promissory estoppel claim alleging that Yahoo had explicitly promised the plaintiff it would remove the content and failed to honor its promise. That claim, this Court explained, could go forward because it imposed a duty "distinct" from a publisher's—a contractual obligation to perform the legal obligations a party voluntarily undertakes. *Id.* at 1107. Yahoo was, therefore, being held liable for its *own* conduct (making and breaking a promise), and not for publishing the speech of others.

2. *Barnes* does not stand alone. This Court has consistently held that Section 230 does not immunize companies for their own conduct. *See, e.g.*, *Lemmon*, 995 F.3d at 1092; *HomeAway.com*, 918 F.3d at 682–83; *Roommates.Com*, 521 F.3d at 1165. And it has repeatedly made clear that this rule applies even where "a cause of action would not . . . have accrued but for . . . third-party content." *HomeAway.com*, 918 F.3d at 682; *see,*

e.g., *Lemmon*, 995 F.3d at 1092; *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016). After all, "publishing content is a but-for cause of just about everything" internet companies are "involved in." *Lemmon*, 995 F.3d at 1093. But, again, Section 230 applies only where the claim "seeks to hold" an internet company "responsible" for publishing that third-party content. *Id.* The relevant question, therefore, is not whether a claim depends on third-party content, but rather whether it seeks to impose on an internet company a "duty" that would "necessarily require an internet company to monitor," edit, or remove that content. *HomeAway.com*, 918 F.3d at 682.

Take, for example, this Court's decision in *Lemmon*, which held that Section 230 did not immunize Snapchat for its design of a cell phone app that encouraged dangerous driving. 995 F.3d at 1091–94. Snapchat had created a speed filter, which allowed users to overlay their real-time speed on top of a photograph, and an incentive system that rewarded users for using the filter at fast speeds. *Id.* at 1088–90. According to the plaintiffs, that encouraged teens to drive dangerously fast—and caused their children's fatal car accident. *Id.* So, the parents brought products liability claims against Snapchat, alleging it negligently designed the app. *Id.*

The Court rejected Snapchat's contention that it was entitled to immunity simply because the "the Parents' claim depends on the ability of Snapchat's users to use Snapchat to communicate their speed to others." *Id.* at 1092. Instead, the Court

examined the duty underlying the products liability claims—that is, the "duty to refrain from designing a product that poses an unreasonable risk of injury or harm to consumers." *Id.* That duty, the Court explained, "differs markedly" from the "duty" of a "publisher," *id.*—that is, "responsib[ility] for . . . content of their publications," Dan B. Dobbs et al., Dobbs' Law of Torts § 478 (2d ed. 2024). *See Lemmon*, 995 F.3d at 1092 ("Snap's alleged duty in this case thus has nothing to do with its editing, monitoring, or removing of the content that its users generate through Snapchat."). That the parents did not, in fact, seek responsibility for content was "further evidenced by the fact that Snap could have satisfied its [products liability duty] without altering the content that Snapchat's users generate." *Id.* All Snapchat had to do was change the speed filter and incentive system that rewarded users for driving at dangerous speeds. *Id.* Thus, the parents "merely [sought] to hold Snapchat liable for its own conduct, principally for the creation of the Speed Filter," and Section 230 immunity was not warranted. *Id.* at 1093.

This Court reached a similar conclusion in *HomeAway.com*. 918 F.3d at 682–83. There, the City of Santa Monica sued online platforms (like AirBnB) that list vacation rentals for violating an ordinance prohibiting them from "processing transactions" for unlicensed properties. *Id.* at 682. The platforms argued that they were entitled to Section 230 immunity because the ordinance "reach[ed] 'publication' activities"—there would be no transactions for the platforms to process if third parties hadn't

posted their vacation rentals. *Id.* at 682. But this Court rejected the platforms' immunity claim. *Id.* at 682–83.

The Court explained that the involvement of "third-party content" is "not enough" to warrant Section 230 immunity. *Id.* at 682. A company is not immune from claims simply because those claims would not have arisen "but for" that content. *Id.* Instead, this Court "look[s] . . . to what the duty at issue actually requires: specifically, whether the duty would necessarily require an internet company to monitor third-party content." *Id.* The ordinance "prohibit[ed] processing transactions for unregistered properties"; it did "not require the Platforms to review the content provided by the hosts of listings on their websites." *Id.* So, this Court held, Section 230 did not apply.

The Court recognized that to comply with the ordinance, the platforms would have to "monitor[] . . . incoming requests to complete a booking transaction" and compare those requests to the City's vacation rental registry. *Id.* But while those booking requests "*result[ed] from* . . . third-party listings," the requests themselves were "distinct, internal, and nonpublic." *Id.* (emphasis in original). That kind of "internal monitoring," this Court held, does not give rise to immunity. *Id.* The Court explained that "[t]he text of [Section 230] is clear that" it does not "declare[] a general immunity from liability deriving from third-party content." *Id.* The statute shields companies from liability for *publishing* third-party content, not for using it. *See*

id. "To provide broad immunity every time a website uses data initially obtained from third parties would eviscerate" the statute. *Id.*

The Court also rejected the platforms' argument that in response to the ordinance, they would have to remove listings for unlicensed rentals because "they cannot leave in place a website chock-full of un-bookable listings." *Id.* at 683. Although removing the listings might be the platforms' "best option from a business standpoint," the Court explained, the ordinance did not *require* them to do so—they could comply without making any "changes to content posted by the website's users." *Id.* "[A]llowing internet companies to claim [Section 230] immunity" from claims that impose no duty to monitor third-party content simply because a company might *choose* to do so would risk "creat[ing] a lawless no-man's-land on the Internet." *Id.* "We have," this Court emphasized, "consistently eschewed an expansive reading of the statute that would render unlawful conduct magically lawful when conducted online, and therefore giving online businesses an unfair advantage over their real-world counterparts." *Id.*

The Ninth Circuit is not alone in holding companies liable for their own conduct. Several other circuits have adopted similar frameworks. *See, e.g.*, *G.G. v. Salesforce.com, Inc.*, 76 F.4th 544, 567 (7th Cir. 2023) (no immunity when claim held defendant liable "for its own . . . acts or practices, rather than for publishing content created by another"); *Henderson*, 53 F.4th at 123 (no immunity unless claim "bases the

defendant's liability on the disseminating of information to third parties" and "imposes liability based on the information's improper content"); *Fed. Trade Comm'n v. LeadClick Media, LLC*, 838 F.3d 158, 176 (2d Cir. 2016) (no immunity when claim held defendant liable for "its *own* deceptive acts or practices," and not "as a publisher or speaker of another's content").

III. Section 230 cannot immunize Grindr for claims based on its own conduct.

The district court held that all of Doe's claims were barred by Section 230 because, "[i]f Grindr had not published [] user-provided content, Doe and the adult men would never have met and the sexual assaults never occurred." Op. 3. In other words, the district court reasoned that immunity was available because publication caused Doe's claims. But as explained above, this Court has repeatedly rejected a but-for causation test for immunity. Instead, it has looked to the specific duty that each claim imposes—and whether that duty requires the defendant to "edit[], monitor[], or remov[e]" content posted by a company's users. *Lemmon*, 995 F.3d at 1092. The district court's failure to adhere to that approach led it to improperly apply Section 230 immunity to the claims here.

Take, for instance, Doe's product liability claims. Doe alleges that Grindr is defective because it matches children with adults for sexual encounters. Compl. ¶¶ 89–115. The claims derive from the "duty to refrain from designing a product that poses an unreasonable risk of injury or harm to consumers"—a duty that "differs

markedly from the duties of publishers as defined in [Section 230]." *Lemmon*, 995 F.3d at 1092. Imposing a duty on Grindr not to match children with adults does not force Grindr to monitor, change, or remove any of the content its users post. Instead, Grindr could avoid liability through, for instance, age verification and geofencing—neither of which has anything to do with user-posted content. *See* Compl. ¶ 107a–c (suggesting a variety of options for compliance).

A duty to verify that a user is over 18 before allowing them to access the app would require Grindr to adopt age verification technology. Compl. ¶¶ 76–77. It would not require Grindr to monitor, change, or remove any of the content posted on the app. In fact, the Fourth Circuit in *Henderson* recently held that a similar duty does not implicate Section 230. *Henderson*, 53 F.4th at 125. There, the plaintiffs claimed that a credit reporting website failed to verify that users complied with the Fair Credit Reporting Act before allowing them to access the site. *Id.* The Court held that the website's argument for Section 230 immunity over this claim was "easily disposed of because liability is in no way based on the improper content of any information spoken or published" by the website. *Id.* It's based solely on the website's duty to verify that its users meet certain legal requirements. Age verification is no different.

The same is true for geofencing. To prevent children from being matched with adults, Grindr could geofence—that is, prevent the app from functioning at—schools. That, too, "has nothing to do with its editing, monitoring, or removing of

the content that its users generate through [Grindr]." *Lemmon*, 995 F.3d at 1092. Indeed, Doe does not allege that users post their geolocations on their profiles or in their messages or that Grindr needs to monitor those profiles and messages. Instead, the complaint makes clear that Grindr knows where users are because the app itself conveys their location to Grindr directly. *See* Compl. ¶¶ 6, 55, 100.

Liability based on Grindr's use (or lack thereof) of geolocation data is therefore no different than the liability this Court approved in *HomeAway.com*: liability for Grindr's own choices about what to do with data it collects. As in *Homeaway.com*, "the only monitoring that appears necessary in order to comply with the [duty] relates to incoming requests" involving "content that . . . is distinct" from user posts (there, requests to book properties for vacation; here, geolocations). *See* 918 F.3d at 682. Section 230 does not preclude "a duty to cross-reference" that content against external databases (there, to cross list the property address in the booking request against the City's registry of licensed properties; here, to cross list geolocations against school addresses). *Id.*

Consider also Doe's negligent misrepresentation claim. That claim implicates Grindr's own conduct as well. Arising from the duty to communicate accurate information, *see* Compl. ¶ 134, the claim seeks to hold Grindr responsible for misrepresenting (for instance, in advertisements, *see id.* ¶¶ 39–40) that the app is safe for children, *see* Compl. ¶¶ 133–42. That's Grindr's own speech and conduct. Indeed,

the company has myriad options available for compliance outside of monitoring its users' content—most obviously, to stop encouraging children on TikTok and Instagram to use an app meant for adults.

Doe's claim that Grindr failed to adequately warn users of the risk of child exploitation targets Grindr's own conduct too. *See* Compl. ¶¶ 116–25. Doe alleges that Grindr learned of these risks from "the numerous articles, court cases, and research regarding child exploitation on Grindr." *Id.* ¶ 118. And indeed, Grindr had to know about the risk of child exploitation—it was actively advertising the sex app to children and thus knew that they might use the app. *Id.* ¶¶ 39, 40. Because knowledge of the risk and thus the duty to warn came from outside sources—and Doe is *not* alleging that Grindr learned about the risk from monitoring users' profiles or private messages—no monitoring of improper user-generated content is involved. Rather, to avoid liability, all Grindr would have to do is issue warning statements through the app.

As these examples demonstrate, Doe's lawsuit seeks to hold Grindr liable for its design choices, its affirmative misrepresentations, and its failure to warn children of known dangers. That's not liability for disseminating the speech of another; it's liability for Grindr's own conduct. Section 230 does not provide Grindr with immunity for these actions.

CONCLUSION

The district court's decision granting Grindr Section 230 immunity for claims targeting Grindr's own conduct should be reversed.

Respectfully submitted,

/s/ Matthew W.H. Wessler
MATTHEW W.H. WESSLER
ALISA TIWARI
GUPTA WESSLER LLP
2001 K Street NW, Suite 850 North
Washington, DC 20006
(202) 888-1741
matt@guptawessler.com

JEFFREY R. WHITE
Senior Associate General Counsel
AMERICAN ASSOCIATION FOR JUSTICE
777 6th Street NW, #200
Washington, DC 20001
(202) 617-5620

Counsel for Amicus Curiae

May 17, 2024

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because this brief contains 4,762 words excluding the parts of the brief exempted by Rule 32(f). This brief complies with the typeface requirements of Rule 32(a)(5) and the type-style requirements of Rule 32(a)(6) because this reply brief has been prepared in proportionally spaced typeface using Microsoft Word in 14-point Baskerville font.

/s/ Matthew W.H. Wessler
Matthew W.H. Wessler