No. 21-1678

In the United States Court of Appeals for the Fourth Circuit

TYRONE HENDERSON, SR., GEORGE O. HARRISON, JR., AND ROBERT MCBRIDE, INDIVIDUALLY AND ON BEHALF OF OTHERS SIMILARLY SITUATED,

Plaintiffs-Appellants,

v.

THE SOURCE FOR PUBLIC DATA, L.P., D/B/A PUBLICDATA.COM, SHADOWSOFT, INC., HARLINGTON-STRAKER STUDIO, INC., DALE BRUCE STRINGFELLOW,

Defendants-Appellees.

On Appeal from the United States District Court
for the Eastern District of Virginia, Richmond Division
No. 3:20-cv-00294-HEH, Hon. Henry E. Hudson

BRIEF FOR THE STATES OF TEXAS, ALABAMA, ARIZONA, ARKANSAS, CONNECTICUT, GEORGIA, IOWA, MAINE, MICHIGAN, MINNESOTA, MISSISSIPPI, NEBRASKA, NEVADA, NORTH DAKOTA, OHIO, SOUTH CAROLINA, SOUTH DAKOTA, UTAH, VERMONT, AND VIRGINIA AS AMICI CURIAE IN SUPPORT OF APPELLANTS

KEN PAXTON
Attorney General of Texas
BRENT WEBSTER
First Assistant Attorney General

Office of the Attorney General
P.O. Box 12548 (MC 059)
Austin, Texas 78711-2548
Tel.: (512) 936-1700
Fax: (512) 474-2697

JUDD E. STONE II
Solicitor General
Judd.Stone@oag.texas.gov
BILL DAVIS
Deputy Solicitor General
KYLE D. HIGHFUL
Assistant Solicitor General

Counsel for Amici Curiae

[Additional counsel listed at end of brief]

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Other Authorities:

Statement of Interest of Amici Curiae

Amici States have an interest in protecting their citizens from unscrupulous website operators that provide criminal-history information with little regard for its veracity. Inaccurate or incomplete information can destroy the reputations of hard-working Americans and cause them undeserved difficulty in finding employment or housing. It can also mean that employers miss out on hiring qualified candidates because online background checks return false positives. Because Defendants propose an overbroad interpretation of the Communications Decency Act that would nullify the protections Congress enacted in the Fair Credit Reporting Act ("FCRA"), this appeal implicates Amici States' common interest. Amici States are authorized to file this brief under Federal Rule of Appellate Procedure 29(a)(2).

Introduction

Inaccurate or incomplete consumer reports have created a nationwide problem. Plaintiffs allege that Defendants willfully ignored federal law and put them and other Virginians at risk for missing out on valuable employment opportunities. In response, Defendants assert that section 230 of the federal Communications Decency Act provides them with absolute immunity from Plaintiffs' suit.

But section 230's text provides no basis for such a sweeping claim to immunity. Justice Thomas recently recognized the need to reevaluate the broad immunity that courts have read into section 230. *See Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 141 S. Ct. 13, 14 (2020) (Thomas, J., statement respecting the denial of certiorari). This case provides an opportunity to define the limits of section 230's

reach. The Court should honor the statute's plain language, reject Defendants' invitation to expand section 230 immunity beyond existing precedent, and reverse the district court's judgment.

STATEMENT OF THE CASE*

I. Defendants Sell Consumer Reports Without Complying with the FCRA.

Defendants conduct an operation that has been ongoing for almost 30 years. Dale Bruce Stringfellow, the scheme's architect, formed ShadowSoft, Inc., in 1993. Joint Appendix ("JA") 22, ¶ 34. Since then, Stringfellow and his shell companies The Source for Public Data, L.P. ("Public Data") and Harlington-Straker Studio, Inc., have profited from compiling and selling public records while seeking to evade state and federal consumer-protection laws. JA.22–28, ¶¶ 34–75. Although based in Texas, Public Data was incorporated in Anguilla after the State responded to complaints about Defendants' website by enacting legislation that threatened Defendants' business model. JA.22, ¶¶ 39–40; JA.24, ¶ 46. Defendants have marketed information obtained from the Texas Department of Transportation. JA.22, ¶ 35. They deny being subject to the FCRA and have made no efforts to comply with it. JA.28, ¶¶ 76–77; JA.33, ¶ 101.

---

* Given the procedural posture, Amici States assume, for purposes of this brief, that Plaintiffs' well-pleaded allegations are true. *See* Fed. R. App. P. 12(c); *Pulte Home Corp. v. Montgomery County*, 909 F.3d 685, 691 (4th Cir. 2018). Amici States take no position on the merits of Plaintiffs' claims.

II. Plaintiffs Have Endured the Consequences of Inaccurate or Incomplete Consumer Reports.

Plaintiff Tyrone Henderson, Sr., has suffered long-standing problems with consumer reporting agencies confusing him with a similarly named person who has a criminal history. JA.35, ¶ 113. He has repeatedly been denied employment because of these inaccuracies. JA.35, ¶ 114. To try to forestall future false reports, Henderson requested a copy of his file from Defendants. JA.35–36, ¶ 116. When they did not respond, Henderson sent two additional requests. JA.35–36, ¶¶ 116–17. Defendants never sent the requested information, but, after his third attempt, Henderson received a letter from Defendants' attorney stating that the FCRA does not apply to them and that they had no record regarding Henderson. JA.36, ¶ 117.

Similarly, Plaintiff George O. Harrison, Jr., requested a copy of his file from Defendants because "other consumer reporting agencies had reported inaccurate or obsolete information about him, resulting in the loss of employment or rental opportunities." JA.36, ¶ 118. Defendants never responded to his request. *Id.*

Plaintiff Robert McBride twice requested his file from Defendants and received no response. JA.37, ¶ 119. In addition, McBride was denied employment as a surveyor after his potential employer purchased a background report on McBride from Defendants. JA.37, ¶¶ 120–23. The report "included numerous entries" describing criminal offenses and suggesting that McBride "had been convicted of each of the offenses listed." JA.37–38, ¶ 124. But "the report was inaccurate and incomplete as it failed to indicate that several of the offenses listed had been nolle prossed." JA.38,

¶ 124. Defendants did not inform McBride that they had provided this report. JA.38, ¶¶ 128–30.

III. Plaintiffs Sued to Vindicate Their FCRA Rights, but the District Court Granted Defendants' Motion to Dismiss.

Plaintiffs sued Defendants as members of a putative class of Virginia consumers alleging that Defendants violated the FCRA. JA.17–18, ¶¶ 14–16; JA.39–45, ¶¶ 132–59. McBride also brought an individual claim. JA.45–46, ¶¶ 160–64. Defendants moved to dismiss Plaintiffs' operative complaint under Rule 12(c), arguing that 47 U.S.C. § 230 bars the claims. JA.80–82; Defs.' Mem. in Support of Mtn. for Judgment, *Henderson v. Source for Pub. Data*, No. 3:20-cv-00294-HEH (E.D. Va. Nov. 16, 2020) ("Dkt. 64"). The district court agreed with Defendants, granted the motion, and dismissed Plaintiffs' claims. *Henderson v. Source for Pub. Data*, No. 3:20-cv-00294-HEH, 2021 WL 2003550, at *6 (E.D. Va. May 19, 2021); JA.83–97. This appeal followed.

Summary of the Argument

I. Section 230 prevents a website operator from being treated as the speaker or publisher of third-party content. 47 U.S.C. § 230(c)(1). And it protects a website operator that makes a good-faith effort to restrict access to objectionable content. *Id.* § 230(c)(2)(A).

Plaintiffs allege that Defendants failed to fulfill their obligations under the FCRA to provide consumer files, give notice, obtain certifications from potential employers, and follow reasonable procedures to ensure the accuracy of their consumer reports. None of those claims relies on treating Defendants as the speakers of a third party's

words. Section 230 is therefore inapplicable here. Plaintiffs' claims seek to hold Defendants accountable for their own allegedly wrongful acts and omissions, not for the speech of others or for Defendants' good-faith attempts to restrict access to objectionable content.

The categorical immunity asserted by Defendants is inconsistent with section 230's plain language, which provides website operators a defense only against claims premised on either (1) third-party speech being attributed to the operator or (2) good-faith efforts to restrict access to objectionable content. Plaintiffs' statutory claims are premised on neither of those things. And the precedent on which Defendants rely arose out of a defamation context in the early days of the Internet and does not require affirmance in this novel context. The Court should decline to read additional immunity into the statute.

II. The proper interpretation of section 230 is more than an academic exercise. The unlawful acts of Defendants and other consumer reporting agencies put millions of Americans at risk of having their reputations and livelihoods impaired by inaccurate or incomplete criminal-background information. Faulty reports also lead employers to reject qualified candidates who could have provided valuable services.

Reading section 230 in a disciplined way and rejecting Defendants' expansive interpretation will not destroy the Internet. Properly interpreted, section 230 provides key protections for online actors without affording them the textually insupportable absolute immunity that many website operators demand. It is possible to protect consumers and further employers' interest in obtaining accurate information

about candidates while ensuring that legitimate online businesses that take good-faith measures to report accurate information can continue to thrive.

ARGUMENT

I. Under the Plain Language of Section 230, the District Court Erred in Granting the Motion to Dismiss.

Section 230 prevents a court from treating a provider of interactive computer services as the publisher or speaker of information provided by another information content provider. 47 U.S.C. § 230(c)(1). And it protects a provider who makes a good-faith effort to restrict access to objectionable content. *Id.* § 230(c)(2)(A). But it does not confer broad immunity on a provider merely because a claim involves third-party content.

Here, Plaintiffs' claims do not require treating Defendants as publishers or speakers of information created by a third party. Instead, Plaintiffs seek to hold Defendants responsible for failing to comply with the FCRA's affirmative requirements. JA.42–46, ¶¶ 140–64. That is, Plaintiffs are not alleging that Defendants are liable for what *third parties* said, but for what *Defendants* did or failed to do. Therefore, section 230 provides Defendants no protection.

A. Section 230 does not bar Plaintiffs' claims.

1. Section 230 provides limited protection from liability for third-party content and good-faith efforts to screen offensive material.

Entitled "Protection for private blocking and screening of offensive material," section 230 limits the liability of providers of an interactive computer service in targeted ways. Its centerpiece is subsection (c), "Protection for 'Good Samaritan'

blocking and screening of offensive material." That subsection provides two key limitations on liability.

First, subsection (c)(1) 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." "That is to say, essential to the analysis of a claim against a service is whether the claim treats the provider as a publisher or speaker of another's words. If so, this law precludes such a cause of action." Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 Harv. J.L. & Pub. Pol'y 553, 563 (2018); *see also Doe v. Internet Brands, Inc.*, 824 F.3d 846, 851 (9th Cir. 2016) (noting that "section 230(c)(1) bars only liability that treats a website operator as a publisher or speaker of content provided by somebody else"); *J.S. v. Vill. Voice Media Holdings, L.L.C.*, 359 P.3d 714, 719 (Wash. 2015) (Wiggins, J., concurring) ("The plain language of subsection 230(c) permits liability for causes of action that do not treat the user or Internet service provider (ISP) as a publisher or a speaker.").

To determine whether subsection (c)(1) applies, a court should therefore consider each necessary element of each of the plaintiff's causes of action. If an element requires treating the defendant as the speaker or publisher of third-party content, subsection (c)(1) provides a defense to the action. But if no element requires such treatment, then allowing the cause of action to proceed is consistent with subsection (c)(1) by its own terms.

Unlike subsection (e)(3), subsection (c)(1) does not confer immunity from suit. That is because, while subsection (e)(3) provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section," subsection (c)(1) merely prohibits a court from treating the defendant in a certain way when determining liability. Nothing in subsection (c)(1) prohibits a plaintiff from bringing a cause of action. *Contra* Dkt. 64 at 1 (Defendants' categorical assertion that section 230 provides immunity from suit).

Second, subsection (c)(2)(A) protects a "provider or user of an interactive computer service" from liability "on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be" objectionable. Similarly, subsection (c)(2)(B) limits liability for "any action taken to enable or make available to information content providers or others the technical means to restrict access to material." By their plain language, these provisions protect only the *restriction*, not the dissemination, of content.

2. Because Plaintiffs' claims neither treat Defendants as speakers or publishers of third-party content nor target a restriction of content, section 230 is inapplicable here.

Plaintiffs bring four claims against Defendants. JA.42–46, ¶¶ 140–64. The claims properly treat Defendants as the operators of a "consumer reporting agency" under the FCRA. And none of the claims requires treating Defendants as speakers or publishers of content produced by third parties or target a restriction of content, making section 230 inapplicable.

a. Defendants collectively operate a consumer reporting agency subject to the FCRA because they, "for monetary fees, . . . regularly engage[] in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties" and use a "means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). Moreover, Defendants are not merely passive conduits for others' speech. It is not as though Defendants operate a message board to which users post disparaging remarks about consumers' personal histories. Rather, Defendants seek out and purchase public records from various sources and manipulate the data to make them more marketable. JA.29, ¶¶ 81–82. According to Plaintiffs, they "distill criminal-history information into glib statements"; "strip out or suppress all identifying information relating to the charges"; and "replace this information with their own internally created summaries of the charges, bereft of any detail." JA.30, ¶¶ 84–86. Plaintiffs further allege that Defendants "actively curate the records to match—in Defendants' own view—the request information provided by the employer." JA.30, ¶ 87. To operate their website's search feature, Defendants are alleged to "affirmatively sort, manipulate and infer information to adapt data results to the requests received." *Id.*

Defendants operate a consumer reporting agency because of the steps they take to procure, manipulate, and market consumer information. That conclusion does not require treating any Defendant as "the publisher or speaker of any information

provided by another information content provider," 47 U.S.C. § 230(c)(1), and it has nothing to do with restricting access to objectionable material, *id.* § 230(c)(2).

b. Nor do any of Plaintiffs' specific claims. *First*, Plaintiffs allege that Defendants violated 15 U.S.C. § 1681g by failing to disclose the contents of their files upon request. JA.42–43, ¶¶ 140–47. No element of this claim requires treating Defendants as publishers or speakers of third-party content. The content of the files is irrelevant. Only the alleged failure to disclose matters. Disclosure would have allowed Plaintiffs to dispute information they believed to be inaccurate. Further, nothing in Plaintiffs' allegations suggests that Defendants refused to disclose the files in a good-faith effort to restrict access to objectionable material. 47 U.S.C. § 230(c)(2)(A). Section 230 therefore does not apply.

Second, Plaintiffs allege that Defendants violated 15 U.S.C. § 1681k(a). That section requires a consumer reporting agency which furnishes a report that may have an adverse effect on a consumer's ability to obtain employment to either (1) notify the consumer or (2) maintain strict procedures designed to ensure that the report's information is up to date. According to Plaintiffs, Defendants failed to provide the notification required by subsection (a)(1) or to maintain the procedures required by subsection (a)(2). JA.43–44, ¶¶ 148–53.

As with Plaintiffs' first claim, a court need not treat Defendants as speakers or publishers of third-party content to find that they failed to notify Plaintiffs of the reported information. When Defendants reported adverse information to potential employers, they triggered a statutory duty to let Plaintiffs know. Defendants failed

to send notice, and it is Defendants' inaction that is the potential basis for liability. The same is true regarding Plaintiffs' allegation that Defendants made no effort to ensure that their consumer reports were up to date. Defendants' potential liability arises because their allegedly lax practices put consumers at risk—not because Plaintiffs seek to hold them responsible for publishing some third-party statement or for blocking objectionable material.

Third, Plaintiffs allege that Defendants violated 15 U.S.C. § 1681b by intentionally failing to obtain the certifications required by section 1681b(b)(1). JA.44–45, ¶¶ 154–59. These certifications from an employer must affirm that the potential employee to be investigated has provided written authorization for the employer to procure a consumer report, 15 U.S.C. § 1681b(b)(2)(A), and that the employer will not use the consumer report in violation of law, *id.* § 1681b(b)(1)(A)(ii). Holding Defendants liable for failing to require these certifications before selling reports does not require treating them as speakers or publishers of the information provided in the reports. The focus of the claim is not that the information in the reports was defamatory, incomplete, or otherwise harmful. Instead, it is that Defendants provided the reports outside of the circumstances allowed by Congress. Again, the content of a report is irrelevant, as the certifications are required even if there is no adverse information in the report. And no restriction of access to obscene or objectionable material is at issue.

Fourth, McBride alleges that Defendants violated 15 U.S.C. § 1681e(b), which provides that, "[w]henever a consumer reporting agency prepares a consumer report

it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." According to McBride, Defendants willfully failed to establish or follow reasonable procedures when they furnished the report about him, costing him a job. JA.38, ¶ 127; JA.45–46, ¶¶ 160–64. This claim does not seek to hold Defendants liable as the speaker of the information contained in the report, and no restriction of access to information is involved. Defendants' alleged fault is that they ignored Congress's command to follow reasonable procedures when marketing personal information that has the potential to destroy a consumer's career or reputation. As with Plaintiffs' other claims, section 230 is inapplicable here.

B. The Court should not further expand its and other courts' already broad interpretation of section 230.

As shown above, the plain language of section 230 renders it inapplicable to Plaintiffs' claims. Defendants nevertheless argued in the district court that section 230 bars the claims because it "grants immunity to interactive computer service providers that would impose liability based on third-party content posted on or communicated through the services." Dkt. 64 at 2. And Defendants insisted that section 230's "favorable policies and related immunity have been broadly interpreted by [this Court] and courts nationwide." Defs'. Reply Mem., *Henderson v. Source for Pub. Data*, No. 3:20-cv-00294-HEH (E.D. Va. Dec. 17, 2020) ("Dkt. 69") at 1. But the decisions on which Defendants rely presented an expansive reading of section 230 not supported by its text, and, in any event, are distinguishable from this case.

Although "courts have built a mighty fortress" protecting website operators "from accountability for unlawful activity on their systems," Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 406 (2017), that fortress rests on a flawed foundation. The expansive-immunity understanding of section 230 comes from a small number of early decisions that arose in a very different historical and legal context. As Justice Thomas recently urged, it is time for courts to reconsider "whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms." *Malwarebytes*, 141 S. Ct. at 14 (Thomas, J., statement respecting the denial of certiorari). This Court's prior decisions have interpreted section 230 more broadly than its text justifies. The Court should decline Defendants' invitation to further expand section 230's applications.

This Court's influential decision in *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), "began a string of broad interpretations" of section 230. Leary, *supra*, at 574. *Zeran* was decided in 1997, when courts still needed to explain what the Internet is. 129 F.3d at 328; *see* Leary, *supra*, at 558 ("The Internet of 1996 is unrecognizable today."). The plaintiff sought "to hold AOL liable for defamatory speech initiated by a third party." *Zeran*, 129 F.3d at 330. Rather than adhere to the statute's text and analyze whether the plaintiff's claim required treating AOL as the speaker or publisher of third-party defamatory speech, the *Zeran* Court repeatedly considered section 230's purported "purpose" and the ills the Court believed would follow if it ruled in the plaintiff's favor. *See, e.g.*, *id.* at 330 (discussing "[t]he purpose of this

statutory immunity"), 331 (discussing "Congress' purpose in providing the § 230 immunity"), 333 (expressing concern over the "practical implications" of liability). The Court expanded section 230's plain meaning, stating—without textual support—that the provision "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Id.* at 330. And it discarded the common-law distinction between "publisher" liability and "distributor" liability, *see id.* at 331–34, a doctrinal shift that Justice Thomas recently questioned, *Malwarebytes*, 141 S. Ct. at 15 (Thomas, J., statement respecting the denial of certiorari).

Courts following *Zeran* have "produced an immunity from liability that is far more sweeping than anything the law's words, context, and history support." Citron & Wittes, *supra*, at 408. "[A]lthough § 230 was never intended to create a regime of absolute immunity for defendant websites," judicial interpretation "has created a regime of de facto absolute immunity from civil liability." Leary, *supra*, at 557. As Justice Thomas put it, "[a]dopting the too-common practice of reading extra immunity into statutes where it does not belong, courts have relied on policy and purpose arguments to grant sweeping protection to Internet platforms." *Malwarebytes*, 141 S. Ct. at 15 (Thomas, J., statement respecting the denial of certiorari) (citation omitted).

As a result, website operators "have been protected from liability even though they republished content knowing it might violate the law, encouraged users to post illegal content, changed their design and policies for the purpose of enabling illegal

activity, or sold dangerous products." Citron & Wittes, *supra*, at 408 (footnotes omitted). In a particularly egregious example, victims of sex trafficking alleged "that Backpage, with an eye to maximizing its profits, engaged in a course of conduct designed to facilitate sex traffickers' efforts to advertise their victims on the website." *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 16 (1st Cir. 2016). The plaintiffs further alleged that "Backpage's expansion strategy involved the deliberate structuring of its website to facilitate sex trafficking," that "Backpage selectively removed certain postings made in the 'Escorts' section (such as postings made by victim support organizations and law enforcement 'sting' advertisements) and tailored its posting requirements to make sex trafficking easier," and that Backpage removed metadata from uploaded photographs to protect traffickers. *Id.* at 16–17. As a result of being trafficked through Backpage, one plaintiff was allegedly raped over 1,000 times. *Id.* at 17.

Yet the court embraced a "broad construction" of section 230 and "a capacious conception of what it means to treat a website operator as the publisher or speaker of information provided by a third party." *Id.* at 19. The court focused on "but-for" causation—that is, there would have been no harm "but for the content of the postings," *id.* at 20—and held that each decision Backpage made, even if intended to facilitate sex trafficking, was undertaken as a "publisher" and therefore entitled to protection under section 230, *id.* at 20–21.

Courts have strayed so far from the statute's text that they now extend immunity to online actors even when the plaintiff is not "trying to hold the defendants liable

'as the publisher or speaker' of third-party content" but only for "the defendant's own misconduct." *Malwarebytes*, 141 S. Ct. at 18 (Thomas, J., statement respecting the denial of certiorari); *see* Citron & Wittes, *supra*, at 413–14 (giving examples of "providers and users whose activities have been immunized or seem likely to enjoy immunity from liability under the broad approach to § 230"). Attorneys general of 44 States, the District of Columbia, and two Territories have pointed out to Congress that courts have interpreted section 230 too broadly and reached "the perverse result" of protecting those who knowingly profit from illegal activity. *See* Letter from Nat'l Ass'n of Att'ys Gen. to Cong. Leaders (May 23, 2019), https://tinyurl.com/naag2019; *see also* Nat'l Ass'n of Att'ys Gen., *State AGs Support Amendment to Communications Decency Act* (May 23, 2019), https://tinyurl.com/naagsite (all cited websites last visited October 15, 2021).

But even accepting the expansive immunity courts have read into section 230 does not require affirmance here. As the district court acknowledged, the application of section 230 to the FCRA "is entirely novel." *Henderson*, 2021 WL 2003550, at *1. *Zeran*, for example, involved only content posted by a third-party to a website hosted by the defendant. 129 F.3d at 328. The *Zeran* Court did not consider the situation presented here, where Defendants allegedly purchased information from third parties, manipulated that information and compiled it into reports, and then sold the reports without complying with statutory certification and notification requirements. As explained above in Part I.A.2, section 230 does not bar Plaintiffs' claims, because they do not require treating Defendants as the publisher or speaker of third-party

content. If Defendants had complied with the FCRA, Plaintiffs may have had the opportunity to discover and correct inaccurate information in their reports, whether the inaccuracies were introduced by Defendants or the public data they collected.

A recent decision of the Supreme Court of Texas, *In re Facebook, Inc.*, 625 S.W.3d 80 (Tex. 2021) (orig. proceeding), is instructive. In that case, human trafficking survivors brought claims for "negligence, negligent undertaking, gross negligence, and products liability based on Facebook's alleged failure to warn of, or take adequate measures to prevent, sex trafficking on its internet platforms." *Id.* at 83. The plaintiffs also brought claims "under a Texas statute creating a civil cause of action against those who intentionally or knowingly benefit from participation in a sex-trafficking venture." *Id.* The Court "agree[d] that Justice Thomas's recent writing lays out a plausible reading of section 230's text," *id.* at 91, but noted that "the broader view of section 230, which originated with *Zeran*, has been widely accepted in both state and federal courts," *id.* at 92. Applying that "broader view," the Texas Court held that section 230 barred the plaintiffs' common-law claims. *Id.* at 93–96. But the Court also held that the plaintiffs' statutory claims could proceed. *Id.* at 96–101. The Court reasoned that the statutory claims did not "treat Facebook as a publisher who bears responsibility for the words or actions of third-party content providers," but instead treated Facebook "like any other party who bears responsibility for its *own* wrongful acts." *Id.* at 98. And the Court found it "highly unlikely that Congress, by prohibiting treatment of internet companies 'as . . . publisher[s],' sought to immunize those companies from *all* liability for the way they run their

platforms, even liability for their own knowing or intentional acts as opposed to those of their users." *Id.*

Like the statutory claims in *Facebook*, Plaintiffs' FCRA claims are far removed from the defamation context of *Zeran* and other seminal section 230 decisions. Plaintiffs' claims turn not on treating Defendants as the speakers of harmful content, but rather as the operators of a consumer reporting agency that has persistently ignored the laws governing its industry. And, unlike the common-law claims in *Facebook* and many prior decisions, the claims in this case do not allege that Plaintiffs were injured by third-party speech but rather by Defendants' inaccurate or incomplete reporting of that information. *See, e.g.*, JA.37–38, ¶¶ 123–24. No third party posted content to Defendants' website. It is Defendants' allegedly manipulated, misattributed, and truncated data, along with their refusal to follow the FCRA's notification and certification requirements, that caused Plaintiffs' injuries, not merely the information Defendants gathered from public records. Section 230 does not "create a lawless no-man's-land on the Internet" where Defendants are immunized merely because they sell consumer reports through a website. *See Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1164 (9th Cir. 2008). Blatant violations of the FCRA "don't magically become lawful" when they occur online. *Id.*

* * *

Section 230 has been applied expansively by this Court and others. But even a broad reading that goes well beyond the statute's text must have its limits, or intentionally unlawful acts perpetrated through the Internet will continue to multiply.

This appeal presents the Court with an opportunity to define section 230's boundaries, curb further expansion, and reject an atextual interpretation that would leave countless consumers at risk by rendering the FCRA toothless.

II. Rejecting Defendants' Overbroad Interpretation of Section 230 Will Protect Consumers and Aid Employers Without Threatening the Digital Economy.

Following the statute's plain text is critical, given the stakes involved in protecting consumers from the reckless dissemination of false or misleading personal information. And rejecting Defendants' broad, atextual claim to immunity will threaten neither the vibrancy of online discourse nor the viability of providing online services.

A. Fidelity to the statutory text will help protect consumers and benefit employers.

Inaccurate and misleading criminal-background reports are a significant nationwide problem. "[A] flawed consumer report can have adverse consequences for both the job-seeking consumer—who loses a conditional offer of employment—and the employer—who rescinds an offer from a potentially valuable and otherwise qualified employee." Noam Weiss, *Combating Inaccuracies in Criminal Background Checks by Giving Meaning to the Fair Credit Reporting Act*, 78 Brook. L. Rev. 271, 273 (2012) (footnotes omitted). "A consumer report can be flawed in two ways: it can attribute an erroneous criminal record to an individual or it can report an individual's criminal record in a flawed manner." *Id.* at 273 n.10. Internet background checks pose unique problems for regulators and consumers. *See* Alexander Reicher, *The Background of*

Our Being: Internet Background Checks in the Hiring Process, 28 Berkeley Tech. L.J. 115, 132–35 (2013).

According to the National Consumer Law Center, "[a]bout 94% of employers and about 90% of landlords use criminal background checks to evaluate prospective employees and tenants." Nat'l Consumer L. Ctr., *Broken Records Redux: How Errors by Criminal Background Check Companies Continue to Harm Consumers Seeking Jobs and Housing* (Dec. 9, 2019), https://www.nclc.org/issues/rpt-broken-records-redux.html. There are "industry-wide" problems with background-screening companies, including the lack of licensing requirements or a central registration system. *Id.* "Anyone with a computer and access to records can start a business," and "[m]any companies attempt to skirt the [FCRA], including by subcontracting work to vendors or disclaiming responsibility." *Id.* Background-screening companies provide reports that "[m]ismatch the subject of the report with another person," "[i]nclude sealed or expunged records," "[o]mit information about how the case was resolved," "[c]ontain misleading information," or "[m]isclassify the offense reported." *Id.* And "[m]any errors are due to common poor practices by background screening companies." *Id.*; *see* Sharon M. Dietrich, *Ants Under the Refrigerator? Removing Expunged Cases from Commercial Background Checks*, Crim. Just. 26, 27–28 (2016). Giving force only to section 230's limited and targeted language will help hold online businesses accountable for carelessly reporting erroneous information that harms both workers and employers across the nation.

B. Fidelity to the statutory text will not endanger freedom of speech or legitimate online business.

In the district court, Defendants praised section 230—or rather their sweeping interpretation of it—for having "paved the way for a free Internet" through its "favorable policies and related immunity." Dkt. 69 at 1. But Defendants' paean obscures the Internet's dark side. Although section 230 "has enabled innovation and expression," "its overbroad interpretation has left victims of online abuse with no leverage against site operators whose business models facilitate abuse." Citron & Wittes, *supra*, at 404.

Section 230 "is a kind of sacred cow—an untouchable protection of near-constitutional status," *id.* at 409, but there is reason to question whether "courts' sweeping departure from the law's words, context, and purpose has been the net boon for free expression that the law's celebrants imagine," *id.* at 410. Scholars have pointed out that a broad interpretation of section 230 can chill speech by protecting those who use online platforms to threaten and harass others into silence. *Id.* at 411. Interpreting section 230 in a manner consistent with its plain language will still provide robust protections to website operators by preventing them from being treated as speakers or publishers of third-party content. *See* 47 U.S.C. § 230(c)(1). Rather than destroying the Internet's free exchange of ideas, a faithful interpretation would foster that freedom by helping make the Internet a safer place to speak.

Nor would rejecting Defendants' expansive reading of section 230 immunity endanger the legitimate online economy. As Justice Thomas has noted, "[p]aring 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." *Malwarebytes*, 141 S. Ct. at 18 (Thomas, J., statement respecting the denial of certiorari). Plaintiffs, including those here, must still prove their cases. *See id.* Honoring Congress's enacted language "will reduce opportunities for abuses without interfering with the further development of a vibrant internet or unintentionally turning innocent platforms into involuntary insurers for those injured through their sites." Citron & Wittes, *supra*, at 423.

Today's "free Internet," Dkt. 69 at 1, provides virtually unlimited access to knowledge, entertainment, and social interaction. But it is also a medium for unlawful and destructive conduct. Properly construing section 230 and allowing Plaintiffs their day in court is one step in nurturing a safer online future for all Americans.

Conclusion

The Court should reverse the district court's judgment and remand the case to the district court for further proceedings.

Respectfully submitted.

Ken Paxton
Attorney General of Texas

Brent Webster
First Assistant Attorney General

Office of the Attorney General
P.O. Box 12548 (MC 059)
Austin, Texas 78711-2548
Tel.: (512) 936-1700
Fax: (512) 474-2697

/s/ Judd E. Stone II
Judd E. Stone II
Solicitor General
Judd.Stone@oag.texas.gov

Bill Davis
Deputy Solicitor General

Kyle D. Highful
Assistant Solicitor General

Counsel for Amici Curiae

STEVE MARSHALL
Attorney General of Alabama

MARK BRNOVICH
Attorney General of Arizona

LESLIE RUTLEDGE
Attorney General of Arkansas

WILLIAM TONG
Attorney General of Connecticut

CHRISTOPHER M. CARR
Attorney General of Georgia

TOM MILLER
Attorney General of Iowa

AARON M. FREY
Attorney General of Maine

DANA NESSEL
Attorney General of Michigan

KEITH ELLISON
Attorney General of Minnesota

LYNN FITCH
Attorney General of Mississippi

DOUGLAS J. PETERSON
Attorney General of Nebraska

AARON D. FORD
Attorney General of Nevada

WAYNE STENEHJEM
Attorney General of North Dakota

DAVE YOST
Attorney General of Ohio

ALAN WILSON
Attorney General of South Carolina

JASON R. RAVNSBORG
Attorney General of South Dakota

SEAN D. REYES
Attorney General of Utah

THOMAS J. DONOVAN, JR.
Attorney General of Vermont

MARK R. HERRING
Attorney General of Virginia

Certificate of Service

On October 15, 2021, this brief was served via CM/ECF on all registered counsel and transmitted to the Clerk of the Court.

/s/ Judd E. Stone II
Judd E. Stone II

Certificate of Compliance

This brief complies with: (1) the type-volume limitation of Federal Rule of Appellate Procedure 29(a)(5) because it contains 5,513 words, excluding the parts of the brief exempted by Rule 32(f); and (2) the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because it has been prepared in a proportionally spaced typeface (14-point Equity) using Microsoft Word (the same program used to calculate the word count).

/s/ Judd E. Stone II
Judd E. Stone II