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 at Richmond
Case No. 3:20-cv-00294-HEH (The Honorable Henry E. Hudson)

REPLY BRIEF OF PLAINTIFFS-APPELLANTS

LEONARD A. BENNETT
CRAIG C. MARCHIANDO
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Boulevard, Suite 1A
Newport News, VA 23601
(757) 930-3660
lenbennett@clalegal.com

KRISTI C. KELLY
KELLY GUZZO PLC
3925 Chain Bridge Road, Suite 202
Fairfax, VA 22030
(703) 424-7570
kkelly@kellyguzzo.com

JENNIFER D. BENNETT
GUPTA WESSLER PLLC
100 Pine Street, Suite 1250
San Francisco, CA 94111
(415) 573-0336
jennifer@guptawessler.com

MATTHEW WESSLER
LINNET DAVIS-STERMITZ
GUPTA WESSLER PLLC
2001 K Street, NW, Suite 850 North
Washington, DC 20006
(202) 888-1741
matt@guptawessler.com

March 7, 2022

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

INTRODUCTION

Nobody asked Public Data to sell background checks online. That, alone, is enough to resolve this case. Section 230 immunizes websites for hosting content *others* seek to make available online—not information an internet company itself decides to post. Public Data does not argue otherwise. It simply ignores the issue entirely. But ignoring Section 230's limitations does not make them go away.

And even if Public Data could wish away Section 230's inapplicability to content the company itself decided to post, that's not enough. Section 230 doesn't offer immunity for content an internet company itself creates or develops, even in part. Public Data cannot dispute that, on the allegations of the complaint, it creates—or, at the very least, develops—the background checks it sells. So, instead, the company ignores those allegations, substituting its own version of the complaint for what the plaintiffs actually wrote. But, as with the statute, ignoring the complaint's allegations doesn't make them go away.

Finally, Public Data retreats to arguing about policy, but there, too, it asks this Court to ignore reality. Public Data does not deny that its position would allow a restaurant to advertise on its website that only white people are allowed, so long as it copies the sign from somewhere else. Nor does it deny that a Facebook user could knowingly defame a political rival, so long as someone else does so first. The company just baldly asserts that those who wish to violate the law online won't take

advantage of this loophole. But Public Data's own efforts to avoid complying with the Fair Credit Reporting Act show otherwise. Denying Public Data immunity for selling background checks online won't, as the company claims, "undermine the functioning of democratic society"—it will simply ensure that companies that sell consumers' personal information to lenders, employers, and landlords comply with the law.

Public Data asks this Court to rewrite the law, rewrite the complaint, and rewrite reality. The Court should decline the invitation.

ARGUMENT

I. The plaintiffs' claims do not seek to hold Public Data liable for performing the traditional functions of a publisher.

Public Data concedes (at 21) that Section 230 only immunizes companies—even publishing companies—from claims that seek to hold them liable for their exercise (or lack thereof) of a publisher's "traditional editorial functions." *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). But it cannot identify a single claim here that does so. No claim in this case asserts, for example, that the company was required to publish or remove a particular background check, monitor the content of its background checks, or alter that content in any way. *See* Opening Br. 19–21. That's unsurprising: The Fair Credit Reporting Act imposes no such requirements. *See id.* at 20–23. It requires that companies disclose files to consumers upon request, notify consumers of sales, require buyers to certify they have a lawful purpose, and

adopt reasonable procedures; it says nothing about publishing information (or not) or monitoring content (or not). *See id.*[1]

So Public Data asks this Court to reinterpret what it means to hold a company liable for the exercise of traditional publishing functions. According to Public Data, it does not mean—as courts have long held—that the claims would impose a duty on the company to monitor or alter the content of its website. Rather, in Public Data's view, claims hold a company liable for traditional publishing functions *any time* the claims "could not have [been] brought" had the company not published something online. Response Br. 21–24. In other words, Public Data argues that Section 230 immunizes an internet company's conduct any time publication is a but-for cause of the plaintiff's claims. *See id.* Because "[p]ublishing activity is a but-for cause of just about everything" internet companies are "involved in," Public Data's approach would immunize websites for virtually anything they do. *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016).

Courts throughout the country—including this one—have already rejected this approach. As this Court has made clear, Section 230 does not provide blanket immunity to companies that publish information online. *See Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 139 (4th Cir. 2019). It immunizes internet companies

[1] Unless otherwise specified, internal quotation marks, citations, emphases, and alterations are omitted throughout the brief. And all citations to the docket are to the district court docket, Case No. 20-cv-00294.

only where the "underpinning" of a plaintiff's claims is the "content of the speech" the company publishes, *id.*—that is, only when the claims seek to impose duties that "necessarily require" monitoring or altering "third-party content," *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019). And the mere fact that publication of information "could be described as a 'but-for' cause" of a plaintiff's injuries" doesn't meet this standard. *Internet Brands*, 824 F.3d at 853.

Judge Niemeyer's recent opinion in *Erie* illustrates the point. There, an insurance company sued Amazon to recoup the payment to its insured after a defective headlamp, purchased from a third-party seller on Amazon's website, caught fire and ignited a house. *Erie Ins.*, 925 F.3d at 138. The insurance company could not have brought the claim had Amazon not published third-party speech—the listing for the headlamp. Yet, the "underpinning" of the claim wasn't the content of this speech; it was Amazon's "actions as a seller (or distributor)" of a defective product. *Id.* at 139. So even though publication was a "but-for" cause of the plaintiff's claims, this Court held that Amazon was not entitled to immunity. *See id.* This is all that's necessary to reject Public Data's novel effort to expand the scope of Section 230 immunity.

And *Erie* has plenty of company. Indeed, courts routinely hold that Section 230 does not offer immunity simply because publication is a but-for cause of a plaintiff's claims. *See, e.g.*, *HomeAway.com,* 918 F.3d at 682 (no immunity even though

"third-party listings" advertising rentals were a "but-for cause" of obligations); *Internet Brands*, 824 F.3d at 853 (no immunity even though "[p]ublishing activity" was "a but-for cause" of plaintiff's claims); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1106–09 (9th Cir. 2009) (no immunity just because claim would not have arisen but for third-party comments posted on a website's message board).

In all of these cases, the plaintiffs' claims did not require the internet company to monitor or alter the content of the speech it publishes—they sought to hold the company liable for its own conduct. And so, in each case, the company's request for Section 230 immunity was rejected—even though publication was a but-for cause of the claim.

So it is here. As in each of these cases, the plaintiffs' claims here are based on Public Data's own conduct—its failure to disclose files upon request, for example, or to require buyers to certify that they have a proper purpose. They do not require the company to monitor or alter the content of the background checks it publishes. To the contrary, Public Data can comply with the obligations the Fair Credit Reporting Act imposes "without" changing the content it publishes at all. *HomeAway.com*, 918 F.3d at 683. Public Data therefore is not entitled to immunity.[2]

[2] Public Data does argue (at 23–24) that, because plaintiff Robert McBride's individual claim under 15 U.S.C. § 1681e(b) requires proof that its background check on him contained inaccurate information, that claim "explicitly seeks to hold Public Data liable for its decision to publish" the background check. That is wrong. As

II. Public Data's background checks were not provided by another information content provider.

Even if Public Data's publisher argument were correct, Section 230 still would not shield the company from liability. Section 230 immunity requires not only that a company be treated as a publisher, but that it be treated as a publisher of "information provided by another information content provider." 47 U.S.C. § 230(c)(1). Public Data assumes (at 27) that this requirement is satisfied whenever an internet company "makes available online lawfully obtained information that was created by a third party." And, the company asserts, that's all it does. It is wrong on both counts.

A. Section 230 does not immunize companies for their own internet posts.

Public Data's entire argument rests on the assumption that Section 230 immunizes internet companies for anything they put online, so long as they "lawfully obtained" it elsewhere—even if nobody asked them to post it on the internet. Response Br. 29. But as the opening brief explains, that assumption is incorrect. *See* Opening Br. 35–38. Section 230 does not immunize all information that happens to come from somewhere else. It only immunizes companies for posting information that *another* information content provider *chose* to make available online. *See id.*

---

explained in the opening brief (at 21–22), the statute does *not* impose liability for publishing inaccurate content. It imposes liability for failing to establish "reasonable procedures." 15 U.S.C. § 1681e(b).

This commonsense understanding is the only plausible interpretation of the statute's text—not to mention its structure and purpose. *See* Opening Br. 35–38 & n.8. It also avoids absurd results. Otherwise, a doctor who "lawfully obtains" confidential medical information from another physician would have immunity for posting that information online. The same would be true of a pundit who reads a newspaper article asserting that a local politician used a racist epithet and decides to reproduce that claim online—even if the pundit *knows* the newspaper's assertion is false.

Public Data offers no response to our statutory argument. The closest it comes is its assertion (at 39) that interpreting the statute this way imposes an additional requirement that "users post information . . . themselves, such as in the case of an online message board." That is wrong. The relevant question is who chose to make the information available online, not who physically posted that information to the internet. *See* Opening Br. 35–38. So if a government agency (or anyone else) asks Public Data to post information online, then that information was "provided by"—it was made available to internet users by—that government agency, even if it is Public Data that physically posts the information. But where, as here, Public Data itself chooses to make the information available online, it is Public Data itself that

has "provided" that information to internet users. Section 230 does not immunize that choice. *See id.*[3]

B. Public Data creates—or, at the very least, develops—the information it sells online.

Even if Section 230 did immunize companies whenever they post verbatim information lawfully obtained from third parties, that's not what Public Data does. Putting aside whether companies "lawfully obtain" information when they acquire it by lying to government agencies, *see* Opening Br. 37–38, Public Data does not simply post verbatim the data it buys. Instead, the company uses the data it buys to create its own background check reports. *See id.* at 9–10, 29–32. The company thus creates—or, at the very least, develops—the information it ultimately sells. It is not, therefore, entitled to Section 230 immunity.

1. Public Data cannot seriously argue that Section 230 immunizes companies that create background check reports and then sell them online. So, instead, Public Data argues that's not what it does. The company contends (at 30) that it doesn't create background checks but rather "allows members of the public to view public

[3] Public Data's assumption that its posting of any information lawfully obtained from a third party is immunized suffers from a second flaw. Section 230 immunity does not apply to information "provided by" just any third party, but only to information provided by "another information content provider"—that is, the creator or developer of the information. 47 U.S.C. § 230. Public Data makes no effort to show that the government agencies and companies from which it acquires information created or developed that information.

records . . . which come directly from various local, state, and federal government agencies, mainly in unaltered form." And because this appeal is from a motion for judgment on the pleadings, Public Data also asserts that this description of its business is alleged in the complaint. *Id.* The problem for Public Data, however, is that the complaint doesn't actually say that; in fact, it says exactly the opposite. *Cf. Burbach Broad. Co. of Delaware v. Elkins Radio Corp.*, 278 F.3d 401, 406 (4th Cir. 2002) (explaining that on a motion for judgment on the pleadings, "we assume the facts alleged in the complaint are true and draw all reasonable factual inferences in [the plaintiff's] favor").

According to the complaint, Public Data *doesn't* simply allow internet users to view public records "in unaltered form." The company *uses* public records—and other data it buys from government agencies and corporations—to create background check reports on individuals, which it then sells to lenders and employers. *See* JA29–30, 37–38. In doing so, it chooses which data should be included in its reports; buys that data from government agencies and corporations; combines it, "parse[s] and limit[s]" it, "distill[s]" it "into glib statements," and summarizes consumers' supposed criminal histories—all to create a new report in a unique "proprietary" format. JA29–31. It even introduces its own inaccuracies along the way, by definition creating information not present in the data it buys—*not* offering that data "nearly verbatim," Response Br. 36. *See* JA37–38.

As a result, this case is nothing like the cases upon which Public Data so heavily relies. The plaintiffs do not seek to hold the company liable for comments posted by consumers, *Nemet Chevrolet, Ltd. v. Consummeraffairs.com, Inc.*, 591 F.3d 250, 252 (4th Cir. 2009), or for making minor edits to "user-created content" posted on its website, *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1169 (9th Cir. 2008) (en banc). They seek to hold Public Data liable for selling background check reports the company *itself* created without complying with the law governing such sales.

As to the *actual* allegations of the complaint, Public Data has virtually nothing to say. The company just repeats (at 38) the incorrect assertion that it is an access software provider. *See* Opening Br. 26. But even if that were true, it's irrelevant. Access software provider or not, Public Data creates the background checks it sells. Section 230, therefore, does not apply.

2. Even if Public Data did not create its background checks, it is certainly "responsible"—at least "in part"—for their "development." *See* Opening Br. 32–33. Public Data does not dispute that, at the very least, a website "helps to develop unlawful content, and thus falls within the exception to Section 230, if it contributes

materially to the alleged illegality of the conduct." *Roommates.Com*, 521 F.3d at 1168; *see* Response Br. 38, 46.[4]

Public Data easily satisfies this standard—even on the company's own version of the facts. There's nothing unlawful about government agencies having data about consumers. What's unlawful is what Public Data does with this data: acquires it from government agencies, aggregates it, and sells it to lenders and employers without complying with the requirements of the Fair Credit Reporting Act. Thus, Public Data not only materially contributes to the unlawfulness alleged here; it is solely responsible for it. It is, therefore, "responsible"—at least in part—for the "development" of the online content it sells.

Public Data resists this straightforward conclusion in two ways. *First*, relying exclusively on the Tenth Circuit's decision in *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009), Public Data suggests that the only illegality that matters is an internet

[4] Public Data argues (at 37) that the plaintiffs waived any argument that it develops information. Not so. The plaintiffs argued that Public Data was itself an "information content provider," because it "is responsible, in whole or in part, for the creation *or development* of information." *See* Dkt. 68 at 23–24 (emphasis added). And they relied on cases in which the defendant "did not passively serve as a conduit, but instead actively gathered *and developed* information." *Id.* (emphasis added). Regardless, this Court has discretion to entertain issues raised for the first time on appeal—discretion that is properly exercised where, as here, the issue is a fully briefed "question of law," the "proper outcome is beyond doubt," and injustice would otherwise result. *Arakas v. Comm'r, Soc. Sec. Admin.*, 983 F.3d 83, 105 (4th Cir. 2020). There's no dispute that a defendant develops information when it renders that information unlawful. That's precisely what Public Data did. This Court should not afford the company immunity for doing so based on a dubious claim of waiver.

company's "convert[ing] legally protected records from confidential material to publicly exposed information." *See, e.g.*, Response Br. 44. *Second*, Public Data argues (at 38) that its conduct is no different than that of an ordinary search engine—so, the argument goes, if Public Data is not entitled to immunity, neither is Google. Both of these arguments fail.

As to the first, Public Data simply misreads *Accusearch*. That decision held that a company that obtained confidential phone records and sold them online was "responsible" for "the development of" the information it sold. *Accusearch*, 570 F.3d at 1198. The court did not hold that the *only* way a company can be responsible for developing information is if it makes confidential information public. The decision itself makes this clear—offering several examples of content "development" that do not involve making public previously confidential information. *See, e.g.*, *id.* at 1199–1200 (explaining that an internet company is "responsible" for "developing" content if it obtains and posts online information that is "inherently unlawful" like child pornography, requires users of a housing-search website to post their illegal, discriminatory housing preferences, or is responsible for inaccuracies in stock quotes it posts). What matters under *Accusearch* is not whether information was confidential before being posted online; what matters is whether the defendant "contributed" to

the "conduct" alleged to be "unlawful." *Id.* at 1200. Public Data indisputably did so here.[5]

And, in any event, the complaint alleges that Public Data's background checks *do* contain legally protected data. *See* JA25–26 (alleging that Public Data acquires legally protected drivers' license information by misrepresenting its purpose for obtaining the records). So even on Public Data's own cramped reading of *Accusearch*, the company has "develop[ed]" the information it sells.

Public Data fares no better arguing that it's akin to an ordinary search engine. Unlike Public Data, ordinary search engines like Google enable users to search information that is *already* online; they do not themselves post the information being searched. And they are "neutral" tools: They "do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends." *Roommates.Com*, 521 F.3d at 1167.

In other words, ordinary search engines do nothing to contribute to the illegality of any search a user might run or the information that search might return. *See id.* The same is presumably true of caselaw-specific search engines like Google Scholar or PACER. Public Data's website, on the other hand, is "designed to achieve

[5] Indeed, elsewhere in its brief (at 46), Public Data itself seems to recognize that, at the very least, development has to encompass any conduct by a defendant that materially contributes to the alleged illegality—not just conduct that makes previously secret information public.

illegal ends," *id.* at 1167—selling consumer reports without complying with the statute that governs such sales. And the information Public Data sells is information the company itself chose to put online—information the company itself rendered both inaccurate and unlawful.

If Google was not a neutral tool, but instead specifically designed to facilitate illegal searches—for instance, if it offered special tools to search for child pornography, or for housing based on race, or if it sold consumer credit information to users without certifying they have a legally proper purpose—it would no longer be entitled to Section 230 immunity. *See id.* Similarly, if instead of returning court records verbatim, PACER sometimes added incorrect, defamatory remarks, it, too, would not be entitled to immunity for doing so. *See id.* Denying immunity to Public Data here does not threaten Google or PACER unless they, too, begin materially contributing to the illegality of the searches users conduct or the information those searches return.

Public Data argues (at 38) that ordinary search engines would *certainly* lose their immunity if this Court took a broader view of web development as meaning making information "usable or available" for publication online, regardless of whether the defendant's actions contributed to the alleged illegality. As an initial matter, this Court need not address this argument. Public Data's actions *do* contribute—in fact, they are solely responsible for—the illegality alleged here. So there's no need for this

Court to decide whether other conduct might also constitute development within the meaning of Section 230.

Moreover, Public Data's argument is wrong even on its own terms. As the opening brief explains (at 32), in the internet context, content development—making information "usable or available" online—refers to "the process of researching, writing, gathering, organizing and editing information for publication on web sites," *Roommates.Com*, 521 F.3d at 1168. And the relevant information is, of course, the information at issue in the lawsuit. *See id.* The information contained in court records is researched, written, and edited by litigants and courts—not PACER. So if a lawsuit challenges the legality of a court record, PACER would have immunity. Similarly, the information on the websites to which Google links is researched, written, gathered, organized, and edited by those sites (or their users)—not Google. Google, therefore, is not responsible for developing that information, and would have immunity from a lawsuit challenging its legality.

Public Data, on the other hand, itself researches, gathers, organizes, and edits the information it sells. And, unlike PACER or Google, Public Data itself chooses to put that information online. Requiring Public Data to abide by the Fair Credit Reporting Act in selling information the company itself chose to put online, therefore, poses no threat to PACER or Google, which do nothing of the kind.

3. In a last-ditch effort to secure immunity, Public Data argues (at 32–35) that its motion for judgment on the pleadings should have been decided on documents *other than* the pleadings. In particular, Public Data asks this Court to consider two document fragments of dubious provenance that the company hand-selected (or, potentially, created) in an effort to prove that the complaint's allegations are wrong. But as the district court explained in rejecting this same request, JA87, documents beyond the complaint may be considered only when they are "explicitly incorporated into the complaint by reference" or when they are "integral to the complaint and there is no dispute about [their] authenticity," *Goines v. Valley Cmty. Servs. Bd.*, 822 F.3d 159, 166 (4th Cir. 2016).

Neither is true here. Public Data doesn't even attempt to argue that these document fragments are incorporated into the complaint—the complaint doesn't mention them. Instead, it argues (at 32–34) that they are somehow integral to the complaint. They are not. Public Data claims these documents are "certain raw data" "previously obtained" (at some unspecified time) from the "Maryland Administrative Office of the Courts" about plaintiff Robert McBride and "screenshots" from a "name search inquiry" on Mr. McBride conducted by a company called "A+ Student Staffing." *See* Dkt. 64-1 at 2. It's unclear what A+ Student Staffing is or how it's relevant to this case. But regardless, the complaint details Public Data's business practices generally. Its allegations do not rely on the results of any single specific

background check. That alone is sufficient to reject Public Data's request. *Cf. Goines*, 822 F.3d at 166 ("[A] document is integral to the complaint where the complaint relies heavily upon its terms and effect.").

Public Data's argument fails for another reason: It ignores the requirement that documents be not just integral to the complaint, but indisputably authentic. *See id.* at 165. Public Data's choice to ignore this requirement is not surprising; the company is unable to demonstrate that the documents *are* authentic. Public Data's declarant did not specify where the documents came from, when they were obtained, how they were obtained, or how they could be verified. *See* Dkt. 64-1 at 2; Dkt. 68 at 10–11 (plaintiffs' opposition to motion for judgment on the pleadings disputing the authenticity of the document fragments).

If Public Data wants a court to decide whether the complaint is accurate, it should move for summary judgment. It may not "transform[]" its motion for judgment on the pleadings into a summary judgment proceeding "featuring a bespoke factual record, tailor-made to suit [its] needs." *Goel v. Bunge, Ltd.*, 820 F.3d 554, 560 (2d Cir. 2016).

And even if this Court were to consider Public Data's document fragments, the outcome here would be no different. At most, these fragments show that in 2016, Public Data created a report on someone named Robert McBride using data from the Maryland courts on someone with the same name. Public Data still cannot

dispute that it chose, of its own accord, to sell this report online—the Maryland courts did not ask it to do so. And the fragments *support* the allegation that Public Data does not simply republish court records. The report Public Data purportedly provided to A+ Student Staffing is *not* just a copy of the "raw data" it purportedly received—it is a report Public Data created. Nor do these document fragments show that Public Data is not responsible for the illegality alleged here: the failure to comply with the Fair Credit Reporting Act.

Public Data is not entitled to transform a motion for judgment on the pleadings into a summary judgment proceeding where only the company submits evidence. But even if it were, this evidence would do nothing to undermine the conclusion that Section 230 does not immunize its conduct.

III. Public Data's policy arguments cannot overcome the text of Section 230 and are, in any event, meritless.

Unable to rely on the text of Section 230, Public Data seeks refuge in policy. But policy, too, cuts against the company's position across the board.

1. Public Data first argues (at 43) that denying it immunity and requiring it—and companies like it—to defend against the FCRA claims here would "undermin[e] the functioning of our democratic society." That is absurd. Our democratic society does not depend on companies like Public Data being able to sell personal information about consumers without complying with the FCRA. If anything, the full participation of consumers in society—the ability to secure housing, credit, and

employment—*depends* on laws like the FCRA, which help ensure that consumer credit information is used in a "confidential and responsible" manner. *Hovater v. Equifax, Inc.*, 823 F.2d 413, 417 (11th Cir. 1987).

Public Data contends (at 42) that "States may well take" a decision denying the company immunity "as an invitation to impose significant obligations on any website that dares to repost public information that the State would rather not see reposted." Of course, as explained above, Public Data does not merely "repost public information." Its business is not making widely available the public documents necessary to a fully-functioning citizenry; it's creating and selling background checks on individual consumers without ensuring that the buyers are legally entitled to receive them.

And it is not Section 230 that prevents states from impermissibly cracking down on speech they don't like. It's the First Amendment. This Court should not expand Section 230 immunity beyond what its text allows merely to provide protection to speech that the Constitution already protects—both online and off.

The point of Section 230 is to ensure that internet companies are not punished for hosting the speech of others; it is not to enable companies to evade laws that govern their *own* conduct simply because they happen to operate online. *See* Opening Br. 3–9, 27–28, 31–33. The only beneficiary of allowing Public Data to do so is Public Data.

2. Public Data next attempts to downplay the consequences of its effort to expand Section 230 immunity to cover anyone who operates online, so long as they get their information elsewhere. But those consequences are an unavoidable result of its interpretation. *See* Opening Br. 34, 36–40.

First, the company argues that allowing it to evade the FCRA will not necessarily mean that other companies follow suit. Most consumer reporting agencies, Public Data asserts (at 43), "create content" by, for example, "assembling information about particular consumers into a consumer file" and "matching records to a specific individual." But that is what Public Data itself does. *See* JA29–31. Indeed, even on Public Data's own account, the whole point of its website is to "match records to a specific individual." *See* Response Br. 10–11 ("Public Data" provides "the records that match" a search inquiry); *id.* at 30. This is not an argument that granting Public Data immunity will not cause harm; it's an argument that Public Data is not entitled to immunity in the first place. We agree.[6]

Next, Public Data claims (at 43–44) that its interpretation of Section 230 would not actually immunize companies for posting information online that wasn't intended for online dissemination. This assertion is perplexing because that's exactly what Public Data itself seeks immunity for here. The company doesn't claim that it

[6] And even if some agencies *also* create credit scores or other assessments, under Public Data's interpretation of Section 230, any that don't are entitled to immunity from any FCRA claims—a breathtaking carveout.

sells background checks at the behest of the government agencies and corporations from which it acquires data—or that those agencies and corporations asked the company to put their data online. Just the opposite. The company proudly trumpets its role in making "difficult-to-find information" accessible. *See, e.g.*, Response Br. 42.

Public Data's actual argument, therefore, is quite narrow: that there's a carveout from Section 230 immunity for internet companies that "convert[] legally protected records from confidential material to publicly exposed information." *Id.* at 44.[7] But this doesn't solve the problem. The repercussions of Public Data's atextual interpretation of Section 230 extend far beyond confidential information. On the company's view, anyone could knowingly post defamatory claims on the internet, so long as they saw them elsewhere first. Restaurants could announce on their website that they serve only customers of a certain race, so long as they do so by copying an announcement that already exists. With the exception, apparently, of information the law requires be kept confidential, anyone could post anything they liked, knowing it violated the law, without consequence—so long as they relied on information that exists elsewhere in doing so.

[7] If the company interpreted Section 230 according to its terms, it would not need to graft onto the statute any special carveouts. As the Tenth Circuit's decision in *Accusearch* makes clear, the reason internet companies that expose otherwise-confidential information lack immunity under Section 230 is because in doing so, they develop that information—not because Section 230 has an unwritten confidentiality exception. *See Accusearch*, 570 F.3d at 1199.

Public Data's only response (at 46) is that "presumably" people wouldn't actually do this; that if someone wanted to violate the law, they'd "create" the exclusionary notice or the defamatory claim themselves. But that makes no sense. "Presumably" if a company or internet user wanted to violate the law, and this Court offered them a loophole through which they could do so with impunity, they would take it. Public Data's own business model proves the point.

By its terms, Section 230 immunizes companies that post information online at the request of others; it does not shield companies for their own choice to make information available. None of Public Data's policy arguments justify departing from the statute's plain text. Indeed, policy considerations only further reinforce the need to adhere to the balance Section 230 strikes. If Public Data believes otherwise, it should direct its arguments to Congress—not this Court.

CONCLUSION

The district court's judgment should be reversed.

Dated: March 7, 2022

Respectfully submitted,

/s/ Jennifer D. Bennett
JENNIFER D. BENNETT
GUPTA WESSLER PLLC
100 Pine Street, Suite 1250
San Francisco, CA 94111
(415) 573-0336
jennifer@guptawessler.com

Matthew W.H. Wessler
Linnet Davis-Stermitz

GUPTA WESSLER PLLC
2001 K Street, NW, Suite 850 North
Washington, DC 20006
(202) 888-1741
matt@guptawessler.com

LEONARD A. BENNETT
CRAIG C. MARCHIANDO
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Boulevard, Suite 1A
Newport News, VA 23601
(757) 930-3660
lenbennett@clalegal.com

KRISTI C. KELLY
KELLY GUZZO PLC
3925 Chain Bridge Road, Suite 202
Fairfax, VA 22030
(703) 424-7570
kkelly@kellyguzzo.com

Counsel for Plaintiffs-Appellants

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 5377 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 brief has been prepared in proportionally spaced typeface using Microsoft Word in 14-point Baskerville font.

/s/ Jennifer D. Bennett
Jennifer D. Bennett

CERTIFICATE OF SERVICE

I hereby certify that on March 7, 2022, I electronically filed the foregoing brief with the Clerk of the Court for the U.S. Court of Appeals for the Fourth Circuit by using the CM/ECF system. All participants are registered CM/ECF users and will be served by the CM/ECF system.

/s/ Jennifer D. Bennett
Jennifer D. Bennett