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. 5 3:20-cv-00294-HEH (The Honorable Henry E. Hudson)

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

October 8, 2021

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

INTRODUCTION

There are hundreds, if not thousands, of consumer reporting agencies—companies that sell information on everything from consumers' credit history to their criminal background to their prescription drug history. The reports these companies provide play a crucial role in nearly every aspect of our lives. Lenders use consumer reports to determine eligibility for auto and home loans; employers use them to vet job applicants; landlords use them to evaluate potential tenants. Because of the far-reaching impact of these reports, Congress passed the Fair Credit Reporting Act to ensure that "consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(4). The statute requires that consumer reporting agencies implement safeguards designed to protect consumers' privacy and their reputations.

Public Data is a consumer reporting agency. It sells background checks online to employers, lenders, and insurance companies—and anyone else willing to pay for them. But it refuses to comply with the Fair Credit Reporting Act. The district court held that it need not do so; that Section 230 of the Communications Decency Act immunizes Public Data from liability. According to the district court, Section 230 protects any company from liability for selling reports online, so long as it creates those reports using data it acquired from others. That describes virtually all consumer reporting agencies. The whole point of a consumer reporting agency is to

aggregate data about consumers from multiple sources into a single report. Thus, the district court's decision essentially exempts wholesale from the Fair Credit Reporting Act any consumer reporting agency that operates online.

But that's not what Section 230 requires. Section 230 protects internet companies from liability when they serve merely as conduits for the speech of their users. Twitter, for example, is not liable for its users' tweets; Facebook is not liable for its users' comments. The statute does not insulate companies from liability for information they themselves decide to post on the internet. And it certainly does not immunize companies for violating the law, simply because they do so online.

Public Data itself creates the background check reports it sells; and Public Data itself decides to post those reports on the internet. Creating and selling consumer reports without complying with the Fair Credit Reporting Act does not suddenly become legal when the reports are sold online. Nothing in Section 230 says otherwise. This Court should reverse.

JURISDICTIONAL STATEMENT

The district court had federal question jurisdiction under 28 U.S.C. § 1331 because this case arises under a federal statute, the Fair Credit Reporting Act, JA42–46. This Court has appellate jurisdiction under 28 U.S.C. § 1291 because this appeal is from a final order dismissing all the plaintiffs' claims with prejudice, JA97. The

district court entered its dismissal order on May 19, 2021. JA97. The plaintiffs timely filed a notice of appeal on June 14, 2021. JA98.

STATEMENT OF THE ISSUE

Does Section 230, 47 U.S.C. § 230(c)(1), immunize Public Data from liability under the Fair Credit Reporting Act simply because the background check reports it creates and sells online rely on data the company purchased from government agencies and other companies?

STATEMENT OF THE CASE

I. Statutory Background

Section 230 was passed in the mid-nineties, when to most people, the internet was "an absolutely brand-new technology." 141 Cong. Rec. H8469 (daily ed. Aug. 4, 1995). But public access to the internet was growing. *See* Susannah Fox & Lee Rainie, Pew Research Center, *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. H8470.[1]

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

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 "endless articles and editorials." Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 Fed. Comm. 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. S9017 (daily ed. June 26, 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. H8469–8472; 141 Cong. Rec. S9017; 141 Cong. Rec. S8293, S8329–48 (daily ed. June 14, 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. S8386 (daily ed. June 14, 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. H8469–72. And, they feared, the criminalization of content based on vaguely-defined terms like "indecent" could amount to broad government censorship. *See id.* at H8470.

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.* "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 themselves, websites and internet service providers, to filter out offensive content—and build tools for parents (and other internet users) to do the same. *See* 141 Cong. Rec. H8469–72. 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, *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). *See id. Stratton Oakmont* relied on a longstanding rule of defamation law that distinguished between distributors and publishers. *Stratton Oakmont*, 1995 WL 323710, at *3. 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, the court held, 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. H8470. 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, s 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). 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 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 content they themselves posted.

II. Factual Background

A. Public Data creates and sells background checks without complying with the Fair Credit Reporting Act.

This case is far removed from anything Congress considered in passing Section 230. Public Data is a background check company. JA15.[2] The company buys personal data about people across the country from government agencies and other businesses—including criminal records, court records, and DMV records. *See* JA25, 31. Much of this data is governed by laws restricting its distribution. *See, e.g.*, 18 U.S.C. § 2721. So Public Data certifies that it is buying the records for its own internal use "to verify the identity of its Customers." JA26. But, in fact, the company uses the records to compile its own "original, proprietary" reports on individuals, which it then sells online to employers, landlords, and lenders seeking background checks. JA30–31. In creating these reports, Public Data does not merely regurgitate the

[2] As explained below, Public Data is controlled through a series of shell companies designed to insulate it from liability. The defendants in this case are Public Data, these other companies, and the person that ultimately controls—and profits from—the enterprise. The defendants act as one in selling background checks through Public Data's website. JA24–25, 27–28. The defendants' motion for judgment on the pleadings treated all of the defendants together, as did the district court's order. *See generally* Dkt. 64; JA89–96. This brief therefore does the same and, unless otherwise specified, refers to the defendants together as Public Data.

records it buys verbatim. Instead, it aggregates the data it acquires, "parse[s]" it, "strip[s] out" much of the information contained in actual court records, and replaces that information with its own "glib" not-always-accurate "statements" purporting to summarize a person's criminal history. JA29–30. Public Data's customers—employers, lenders, insurance companies, landlords—then use these reports to make crucial decisions on everything from hiring to renting to creditworthiness. JA31.

Background screening, like that provided by Public Data, is a multi-billion-dollar industry. JA21. Over ninety percent of employers and landlords use background checks to evaluate prospective tenants and employees. JA20. A background check error, therefore—a false criminal conviction, for example—can make it impossible to find work or housing. JA20.

For that reason, the Fair Credit Reporting Act requires that companies that provide background checks (and other consumer reports) follow procedures designed to ensure that consumers are aware of the information being provided to employers and landlords about them; that employers that buy this information have consent to do so; and that the information consumer reporting agencies sell is as accurate as possible. *See* 15 U.S.C. §§ 1681g, 1681k(a), 1681b(b)(1), 1681e(b).

But Public Data would prefer not to comply with the Fair Credit Reporting Act. Rather than implement the procedures required by the statute, Public Data has

instead structured its business to avoid liability. Initially, the company moved off-shore with the express purpose of avoiding state and federal law. JA23–24. Now, the company has returned to the United States, but it is owned and operated through a series of shell companies designed to ensure that the companies' ultimate owner—Dale Stringfellow—retains the millions of dollars in revenue Public Data generates, while leaving Public Data itself judgment-proof. JA24–25, 27–28.

There have been several lawsuits against Public Data for its failure to comply with the Fair Credit Reporting Act. JA31–32. The Consumer Financial Protection Bureau has investigated the company. JA32. The state of Texas *passed a law* because of complaints about Public Data, attempting to limit companies' ability to disclose personal data purchased from the state. JA22. Even so, Public Data continues to create, market, and sell its background check reports—without complying with state or federal law governing such conduct.

B. This lawsuit.

Tyrone Henderson, George Harrison, and Robert McBride are Virginians who have lost housing or employment opportunities because of inaccurate information reported about them in their background checks. JA35–37. Background checks on Mr. Henderson, for example, often report that he has criminal history which is not, in fact, his, but rather that of another person with a similar name. JA35.

Public Data's background check for Mr. McBride listed multiple criminal offenses, for which he was never actually prosecuted. JA37–38.

In an attempt to determine whether their background checks were accurate, Mr. Henderson, Mr. Harrison, and Mr. McBride each requested a copy of their files from Public Data. JA42. Although the Fair Credit Reporting Act requires consumer reporting agencies to provide consumers' files upon request, 15 U.S.C. § 1681g, Public Data refused. JA42. The company also did not notify Mr. McBride when it provided its (inaccurate) background check to a potential employer—despite the Fair Credit Reporting Act's requirement that it do so, 15 U.S.C. § 1681k(a). JA43. And Public Data does not require that employers certify that they have the permission of the person whose background check they're seeking to procure, nor does it require employers to certify that the information will not be used in violation of the law—even though the Fair Credit Reporting Act prohibits selling background checks to employers without these certifications, 15 U.S.C. § 1681b(b)(1). JA44.

Mr. Henderson, Mr. Harrison, and Mr. McBride, therefore, sued Public Data for its violations of the Fair Credit Reporting Act. They sought to remedy Public Data's misconduct, not just on behalf of themselves, but on behalf of all Virginia consumers who suffered the same harm. JA42–45. The class claims did not target the content of Public Data's background checks. Instead, they sought to hold Public Data liable for failing to comply with the procedures required by the Fair Credit Reporting

Act: the statute's requirement that a consumer reporting agency provide a copy of a consumer's file upon request; that it notify consumers when providing a background check to an employer; and that it require employers to certify that they have permission and will comply with the law before selling them a background check. *Id.* Mr. McBride also alleged an individual claim against Public Data for failing to establish or follow "reasonable procedures to assure maximum possible accuracy" in the report it sold to an employer about him. JA45.

In response, Public Data moved for judgment on the pleadings, arguing that it is immune from liability under Section 230, which provides: "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," 47 U.S.C. § 230(c)(1). *See generally* Dkt. 64. The district court granted Public Data's motion. JA96. Although Section 230 only provides immunity from claims that treat an internet company as the publisher or speaker of third-party content, the district court did not analyze the plaintiffs' specific claims at all. Instead, it categorically asserted—without explanation—that the plaintiffs seek to hold Public Data liable for the content of its reports. JA92.

The court then went on to hold that Section 230 provides Public Data immunity from the plaintiffs' claims for three reasons. First, the court concluded that Public Data is an interactive computer service. JA94. Next, it held that the company

satisfies the statutory definition of an "access software provider"—a specific kind of interactive computer service—and therefore, it is not an "information content provider." JA94–95. The court did not explain how this conclusion could be reconciled with this Court's case law making clear that an interactive computer service can *also* be an information content provider. *See, e.g.*, *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009). And finally, although, by its terms, Section 230 immunity does not apply to companies that "creat[e] *or develop*[]" the offending content, 47 U.S.C. § 230(f)(3) (emphasis added), the court held that to defeat Section 230 here, the plaintiffs were required to "allege that the defendant *created* the content at issue." JA95 (emphasis added). In the district court's view, because the plaintiffs allege that Public Data uses records it buys from other companies and government agencies to create its background check reports, they have not alleged that Public Data created content at all. JA95–96.

SUMMARY OF ARGUMENT

I. Section 230 precludes claims only if they would impose liability on an internet company for performing the traditional functions of a publisher—such as deciding whether to publish, edit, or withdraw from publication third-party speech. The claims here do not seek to hold Public Data liable as a publisher. They do not seek to impose upon Public Data an obligation to publish or not publish third-party speech. They require only that Public Data comply with the procedures mandated

by the Fair Credit Reporting Act—procedures that have nothing to do with the content of the background check reports Public Data sells.

II. Even if the plaintiffs' claims did seek to impose liability on Public Data as a publisher, Section 230 still would not immunize Public Data from those claims. That's because Section 230 applies only to claims that seek to hold an internet company liable as the publisher or speaker of "information provided by *another* information content provider." 47 U.S.C. § 230(c)(1) (emphasis added). And Public Data's background checks are not provided by another information content provider—they are provided by Public Data itself.

A. In holding otherwise, the district court assumed that an interactive computer service could not also be an information content provider. That's incorrect. This Court's case law and the statute itself make clear that an internet company that creates or develops, even in part, the information it posts is an information content provider—even if it is also an interactive computer service.

B. The district court also assumed that an internet company that uses third-party data to create its content is not an information content provider. That, too, is wrong. An internet content provider is "*any* person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet." 47 U.S.C. § 230(f)(3) (emphasis added). There is no exception for companies that rely on third-party data in doing so. Public Data "create[s]" the

background check reports it sells. It is, therefore, an internet content provider and not entitled to immunity.

Even if Public Data did not create the reports it sells, it certainly "develop[s]" them—at least "in part," *id.* In this context, to develop means to make usable or available. That is exactly what Public Data does: It makes available to its customers personal information about consumers they would not otherwise have access to. Public Data also develops the content it sells by "materially contribut[ing]" to its illegality, *Nemet*, 591 F.3d at 257. Indeed, to the extent the claims here can be understood to be based on Public Data's content at all, it is Public Data that is solely responsible for making that content illegal because it is Public Data that is solely responsible for selling its background checks in violation of the Fair Credit Reporting Act.

Finally, even if Public Data neither created nor developed its content, it *still* would not be immune from the plaintiffs' claims because the "information" it publishes is not "provided by another information content provider," 47 U.S.C. § 230(c)(1). Information is only "provided by another information content provider" within the meaning of Section 230 if it is made available by another information content provider to internet users. Here, the only company that made the background check reports Public Data sells—or the data those reports rely on—available to Public Data's users is Public Data itself.

III. Section 230 "was not meant to create a lawless no-man's-land on the Internet." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1164 (9th Cir. 2008). If Congress wanted to create a broad exemption to the Fair Credit Reporting Act for companies that operate online, it would have said so. It did not do so. Courts have repeatedly held that companies like Public Data are not exempt from the law simply because they operate on the internet. This Court should do the same.

STANDARD OF REVIEW

This Court "review[s] de novo the district court's ruling on a motion for judgment on the pleadings." *Pa. Nat'l Mut. Cas. Ins. Co. v. Beach Mart, Inc.*, 932 F.3d 268, 274 (4th Cir. 2019). In doing so, the Court must "assume the facts alleged in the complaint are true and draw all reasonable factual inferences in [the plaintiffs'] favor." *Burbach Broad. Co. of Del. v. Elkins Radio Corp.*, 278 F.3d 401, 406 (4th Cir. 2002).

ARGUMENT

Section 230 does not grant blanket immunity to any company that happens to operate online. A defendant can seek refuge in Section 230 only if (1) it is the "provider or user of an interactive computer service"; and (2) the plaintiffs' claims require it to "be treated as the publisher or speaker of any information" that (3) is "provided by

another information content provider." 47 U.S.C. § 230(c)(1).[3] Public Data claims to be the "provider" of an "interactive computer service"—a system that "enables computer access by multiple users to a computer server," *id.* § 230(f)(2). Dkt. 64, at 10.[4] But that is not enough. Even if that claim were true, Public Data cannot satisfy the other two requirements for Section 230 immunity. The plaintiffs' claims do not require treating Public Data as a publisher or speaker. And they certainly do not require treating Public Data as the publisher of information "provided by *another* information content provider."

Public Data creates the background reports it sells on its website. And it sells them without complying with the procedures required by the Fair Credit Reporting Act. Indeed, its entire business model is designed to evade the statute. Section 230 does not immunize this conduct merely because Public Data provides its background reports to its customers through the internet, rather than by mail.

---

[3] The district court's articulation (at JA92–93) of the requirements to invoke Section § 230 is incorrect. The court stated, for example, that a defendant is immune if it "is alleged to be a creator of the content." JA92–93. That's backwards: A defendant is not immune, if, as here, it creates the content on its website. *See Nemet*, 591 F.3d at 254.

[4] Even this claim is dubious, at best. There is nothing "interactive" about Public Data's website. It does not, for example, host a bulletin board or a comments section or any other forum where users can interact. It's merely a portal through which Public Data sells its background checks to its customers.

I. The plaintiffs' claims do not seek to hold Public Data liable as a publisher.

As this Court has explained, Section 230 precludes claims only if they "would place a computer service provider in a *publisher's* role" *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (emphasis added).[5] Thus, "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter" a third party's speech are prohibited. *Id.*; *see Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 139 (4th Cir. 2019). But lawsuits seeking to hold an internet company liable for *its own* conduct—conduct that has nothing to do with the "publication of another's speech"—are not. *Id.*

The claims here do not seek to hold Public Data liable as a publisher. Public Data *isn't* a publisher—at least not with respect to its background check reports. *See* JA29–31 (explaining that Public Data creates the reports it sells). Public Data is not akin to a magazine or a newspaper or even a public bulletin board. It does not post background check reports to its website, so that any visitor can read them. *See* JA29–30 (explaining that Public Data sells reports to paying customers in response to their

[5] Section 230 also precludes claims that treat an interactive computer service as the speaker of content posted by someone else, but that's not at issue here. The district court concluded that Public Data is a publisher. And, in any event, speaker immunity would fail for the same reasons publisher immunity fails: The plaintiffs do not seek to hold Public Data liable for the content it posted on its website, but rather for its failure to follow the procedures mandated by the Fair Credit Reporting Act.

queries). It does not make its reports "generally known" or "disseminate [them] to the public." Publish, *Merriam-Webster's Collegiate Dictionary* 944 (1994)). It creates and (privately) delivers reports on people to paying customers who ask for them; it simply happens to do so through an internet portal. That is not what the word "publisher" ordinarily means. *See id.*

But even if Public Data were a publisher, that is not enough. The plaintiffs' claims would have to *depend* on the company's status as a publisher; that is, they would have to seek to hold Public Data liable for the "content" of "another's speech" it chose to publish. *See Erie*, 925 F.3d at 139. Put another way, the "duty" a claim seeks to impose would have to "*necessarily* require an internet company to monitor third-party content." *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019) (emphasis added); *cf. id.* (explaining that, even where monitoring third-party speech "would be the best option" for complying with a regulation, the regulation does not treat an internet company as a publisher if there are other methods of compliance that do not require such monitoring).

None of the claims here would "necessarily require" Public Data to monitor *any* content—third-party or otherwise. The plaintiffs allege three claims on behalf of a class: (1) that Public Data failed to disclose their files upon request and notify them of their rights, JA42; (2) that the company failed to notify them when it sold reports about them to employers, JA43; and (3) that the company failed to require that

employers certify that they have consent to procure a background check and will use it only for legal purposes, JA44. The obligations imposed by these claims are, therefore, (1) providing consumers a copy of their file; (2) notifying them when their files are sold; and (3) requiring that employers certify they have consent to procure a background check and will use it legally.

None of these duties implicate the traditional functions of a publisher. None of them require, for example, that Public Data publish third-party speech, remove such speech, or monitor anything posted on its website. *See Zeran*, 129 F.3d at 330. To the contrary, Public Data can comply with its obligations "without" making any "changes to" its content at all, *HomeAway.com*, 918 F.3d at 683. The class claims, therefore, do not seek to impose publisher liability on Public Data. *See id.* And, thus, Section 230 does not apply. *See id.*; *See Erie*, 925 F.3d at 139; *Zeran*, 129 F.3d at 330.

In addition to the class claims, named plaintiff Robert McBride also alleges an individual claim against Public Data for failing to "establish or to follow reasonable procedures" to avoid selling inaccurate consumer reports. JA45. Even this claim, however, does not require Public Data to monitor its content. If the Fair Credit Reporting Act required that reports sold by consumer reporting agencies actually *be* accurate, then, perhaps, adhering to that mandate might require Public Data to monitor the content of its background reports. But the statute imposes no such requirement. *See Henson v. CSC Credit Servs.*, 29 F.3d 280, 284 (7th Cir. 1994). Instead,

the law is clear that the Fair Credit Reporting Act "does *not* require error free consumer reports." Statement of General Policy or Interpretation: Commentary on the Fair Credit Reporting Act, 55 FR 18804-01 (emphasis added). That is, the statute does not impose liability based on the content of a report. Rather, it requires only that consumer reporting agencies adopt "reasonable *procedures*" in compiling the reports they sell. 15 U.S.C. § 1681e(b) (emphasis added). Thus, like the class claims, Mr. McBride's individual claim does not require Public Data to monitor any content.

And it certainly does not require Public Data to monitor "a *third party's* speech," *Erie*, 925 F.3d at 139 (emphasis added). None of the plaintiffs' claims do. Public Data's background reports are Public Data's speech. JA29–31. They are not created by a third party; they are created by Public Data itself. *See id*. Even claims based on their content, therefore, would not require Public Data to monitor third-party speech.

In holding to the contrary, the district court's analysis was limited to a single conclusory sentence: "Plaintiffs here seek to hold Defendants liable for the content on their website." JA92. But, again, that's simply not true. The plaintiffs do not seek to hold Public Data liable for the content of the background reports it sells. They seek to hold Public Data liable for failing to comply with the procedures required by the Fair Credit Reporting Act in selling those reports. For that reason alone, Section 230 does not apply. *See Erie*, 925 F.3d at 139–40 (lawsuit did not treat Amazon as a

publisher or speaker because there was "no claim made based on the content of speech published by Amazon—such as a claim that Amazon had liability as the publisher of a misrepresentation of the product or of defamatory content").

II. Public Data's background reports are not provided by another information content provider.

Even if the plaintiffs' claims did require treating Public Data as a publisher, Section 230 still would not protect the company from liability here. Section 230 does not bar *every* claim that treats an internet company as a publisher. It bars only those claims that treat internet companies as the publisher of "information provided by *another* information content provider." 47 U.S.C. § 230(c)(1) (emphasis added). After all, the statute's purpose is not to immunize companies for their own speech; it's to protect companies that serve as the conduits for the speech of others. *See Nemet*, 591 F.3d at 254. Thus, whether an "interactive computer service" is liable for the content it publishes "turns on" whether it is "also an information content provider." *Id.*

Section 230 defines an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3). Thus, an internet company that "merely enables" its users to post content online is not an information content provider. *Nemet*, 591 F.3d at 254. But a company that creates or develops, at least in part, the content it publishes is; and that company is therefore liable for that content. *Id.*

The content Public Data sells are background check reports. But Public Data is not simply a conduit for these reports; it does not "merely enable" users to post on Public Data's website background checks users themselves have created. The company does not "enable" users to post anything at all. To the contrary, Public Data itself creates the background check reports it sells; and Public Data itself provides those reports online to its customers. *See* JA29–31. It is therefore Public Data that is the information content provider of these reports. *See Roommates.Com*, 521 F.3d at 1162 ("[A]s to content that it creates itself, or is responsible, in whole or in part for creating or developing, the website is also a content provider.").

In holding otherwise, the district court made two fundamental mistakes: *First*, the court assumed that an interactive computer service cannot also be an information content provider. *See* JA94–95. Because, in the district court's view, Public Data satisfied the definition of an "access software provider"—a kind of interactive computer service—the court believed that it could not be an information content provider. *See* JA94–95. *Second*, the court believed that to defeat Section 230 immunity "a plaintiff must allege that the defendant *created* the content at issue"—and that because Public Data uses records it acquires from third parties to create its reports, the company does not, in fact, create any content at all. JA95–96 (emphasis added).

The district court was wrong on both counts. An access software provider, like any other interactive computer service, can also be an information content provider.

And an internet company is an information content provider if it "is responsible, in whole or in part, for the creation *or development* of" internet content. 47 U.S.C. § 230(f)(3) (emphasis added). A company is no less responsible for creating or developing the content it sells simply because it used data it bought from third parties to do so.

A. An interactive computer service can also be an information content provider.

This Court has long recognized that a company can be both an interactive computer service and an information content provider. *See, e.g.*, *Nemet*, 591 F.3d at 254. Indeed, immunity under Section 230 "*turns* on" whether an interactive computer service is "also" an information content provider. *Id.* (emphasis added). That's what the statute's text mandates: Section 230 prohibits treating an interactive computer service as the publisher of information provided by "*another* information content provider." 47 U.S.C. § 230(c)(1) (emphasis added). This prohibition would make no sense if an interactive computer service could not itself be an information content provider.

Nor would treating these two categories as mutually exclusive accord with how the internet actually works. Virtually all websites are both "providers or users of an interactive computer service" *and* "information content providers." Even websites like Twitter, which exist primarily as a conduit for others' speech, are also information content providers with respect to some content. The terms of service on

Twitter's website, for example, were presumably created by Twitter itself. That content, therefore, is not "provided by another information content provider," 47 U.S.C. § 230(c)(1). Twitter itself is the information content provider. To conclude that "interactive computer service" and "information content provider" are mutually exclusive categories, therefore, is not only countertextual; it's counterfactual.

Contrary to the district court's conclusion, the statute's reference to an "access software provider" does not change this analysis. As an initial matter, Public Data is not an "access software provider." To be an "access software provider," a company has to actually provide "software"—or other "enabling tools"—that "filter, screen, allow, or disallow content"; "pick, choose, analyze, or digest content"; or "transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." 47 U.S.C. § 230(f)(4). In lay terms, access software providers are companies that provide tools to users to filter internet content for themselves—by, for example, blocking pornographic content, offensive terms, or computer viruses. *See Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 (9th Cir. 2009).

Public Data sells background checks. The complaint never alleged, and Public Data has never argued, that the company provides software (or any other tools) that enable users to filter internet content for themselves.[6] But even if it had, that would

[6] The district court held that Public Data is an "access software provider" because, in creating its reports, the company "pick[s], choose[s], analyze[s], or

be irrelevant. An "access software provider" is just a type of interactive computer service. 47 U.S.C. § 230(f)(2). And, as explained above, an interactive computer service can also be an information content provider. Thus, the question is not whether Public Data is an access software provider *or* an information content provider. The question is whether Public Data is an information content provider with respect to the background check reports upon which the plaintiffs' claims are based. Because Public Data creates those reports, there should be no doubt that it is. *See, e.g.*, *Roommates.Com*, 521 F.3d at 1162 (where website itself creates content, it is internet content provider); *Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837, at *13 (N.D. Cal. Aug. 16, 2021) (website that creates dossiers of personal information on individuals, using data from third parties, and sells them over the internet is internet content provider).

B. Public Data's background checks were not provided by another information content provider, just because the company used data it bought from other sources in its reports.

Courts routinely hold that Section 230 does not immunize an internet company for its own content just because it used "data initially obtained from third

---

digest[s] content"—the records it buys from government agencies and other companies. JA95. The court appears to have misread the statute. An access software provider is not a company that *itself* picks, chooses, analyzes or digests data in order to create content that it then provides over the internet; it is a company that provides "software" or other "tools" that enable *others* to screen content already on the internet. 47 U.S.C. § 230(f)(4). Public Data does not provide any such tools.

parties" to create that content, *Roommates.Com*, 521 F.3d at 1171. *See, e.g.*, *id.*; *Fed. Trade Comm'n. v. Accusearch Inc.*, 570 F.3d 1187, 1198 (10th Cir. 2009); *Brooks*, 2021 WL 3621837, at *13. And with good reason: Permitting internet companies to evade liability, merely because the content they post online relies on data procured elsewhere, "would eviscerate" the limitation Congress placed on Section 230 immunity—that it does not apply where an internet company itself creates or develops, even "in part," the unlawful content. *Roommates.Com*, 521 F.3d at 1171. Companies that develop and post content using third-party data are still themselves developing and posting content; that is, they are still information content providers. *See id.* The district court's conclusion to the contrary conflicts with years of precedent—as well as the text, structure, and purpose of Section 230.

1. As an initial matter, the district court got the definition of "information content provider" wrong. The court held that "a plaintiff must allege that the defendant created the content at issue." JA95. But that's not what the statute says. The statute defines an internet content provider as "any person or entity that is responsible, in whole or in part, for the creation *or development* of information provided through the Internet." 47 U.S.C. § 230(f)(3) (emphasis added). Thus, even if Public Data did not *create* its background check reports, it is nevertheless an information content provider if it "is responsible" for their "development," even "in part."

2. The district court then applied its incorrect definition incorrectly. The court asserted that "[t]here is no doubt that" Public Data does "not create the content" it sells because the data contained within Public Data's background check reports—for example, whether a person has a criminal conviction—is "derived" from the records the company purchases. JA96. The district court's own explanation demonstrates its error. As the court itself recognized, the content Public Data sells—background check reports—is *not* the same as the data it buys to create that content. Some of the facts in the reports may be "derived" from records the company purchases, but the reports themselves are Public Data's own creation. JA29–31. The company chooses what data those reports should contain; it buys records from government agencies and companies across the country to procure that data; it aggregates the data it buys; "parse[s]" it; summarizes it, including characterizing people's criminal history with "glib statements" that appear nowhere in the records it purchases; and puts all of this together into an "original" report, complete with a "proprietary format" designed to "meet what it perceives to be its clients' needs." *See* JA29–31. The background check reports Public Data sells would not exist if Public Data did not make them. Public Data thus *creates* those reports. *Cf.* Create, *Merriam-Webster's Collegiate Dictionary* 274 (1995) (defining "create" as "to bring into existence" or "invest with a new form . . .").

Common sense reinforces this basic point. If a student writes a history report, they will, of course, rely on facts they gather from other sources. But it is still the student who created the report—not the encyclopedia the student used when researching. So it is here. Public Data procures records from the Maryland Administrative Office of the Courts and the Florida DMV and Texas's Department of Public Safety (and a host of other places). JA26; Dkt. 64 at 3–5. But the Florida DMV does not "creat[e]" the background check reports Public Data sells. Public Data does. That is all that's necessary to understand how the district court went astray. Section 230 does not, as the district court seemed to think, immunize internet companies any time their content includes data "derived" from records purchased from third parties. It immunizes companies only if they did not themselves "creat[e] or develop[ ]," even "in part," the "information" they provide. 47 U.S.C. § 230(f)(3).

As the district court understood it, although Public Data creates background check reports, it does not create "information," because it does not create its own data. *See* JA96. In other words, the court assumed that "information" must mean data or facts. But, particularly in the context of computers and the internet, the aggregation, organization, and summary of data has long been understood to be "information" different from the raw data itself. *See e.g.* Information, *Webster's New World Dictionary of Computer Terms* 205 (1992) (defining "information" as "[p]rocessed data; data that is organized, meaningful, and useful"); Information, *Webster's Computer*

Dictionary 110 (1994) ("a compilation of data"); Information, *Microsoft Press Computer Dictionary* 249 (1997) ("Data consists of facts, which become information when they are seen in context and convey meaning to people.").

More importantly, defining "information" for purposes of Section 230 to mean solely facts or data would vitiate the statute. Section 230 only provides immunity in the first place for claims that treat an internet company as the publisher of "*information* provided by another information content provider." 47 U.S.C. § 230(c)(1) (emphasis added). If information were narrowly defined to mean just data, Section 230 would not apply at all to anything that isn't factual—pornography, for example, or Facebook messages between friends. That would eviscerate the statute. The whole point of the law is to protect users and providers of interactive computer services from liability for internet speech that isn't theirs; if the only speech to which it applies are facts, wide swaths of the internet—including pornography, the content of most concern to the Congress that passed Section 230—would be excluded. Presumably, that's why this Court—and courts around the country—have universally understood the term "information" within Section 230 to mean simply content. *See, e.g.*, *Nemet*, 591 F.3d at 254; *Accusearch*, 570 F.3d at 1201; *Roommates.Com*, 521 F.3d at 1175.[7]

[7] Even if "information" could be defined narrowly to mean facts or data, Public Data still would be responsible—at least in part—for creating the content it publishes. Many of the "facts" contained in Public Data's reports bear little resemblance to the facts contained in the records Public Data buys. For example, the

Bottom line: Public Data creates its background check reports. Contrary to the district court's conclusion, therefore, Public Data creates its content.

3. Even if Public Data did not create the content it sells, it certainly "develop[s]" that content—at least "in part," 47 U.S.C. § 230(f)(3). As we explained above, the district court lost sight of this key second part of the statute's definition of information content provider, ignoring it entirely. As multiple courts have explained, to "develop," in this context, means to "mak[e] usable or available." *See, e.g.*, *Roommates.Com*, 521 F.3d at 1168 (quoting *Webster's Third New International Dictionary* 618 (2002)); *Accusearch*, 570 F.3d at 1198. That is exactly what Public Data does: It makes usable to its customers personal information about consumers they otherwise would not have easy (or any) access to. And web content development, more generally, is typically understood to mean "the process of researching, writing, gathering, organizing and editing information for publication on web sites"—again, precisely what Public Data does. *Roommates.Com*, 521 F.3d at 1168.

At the very least, an internet company develops content within the meaning of Section 230 if it "materially contribut[es]" to that content's illegality. *See Nemet*, 591 F.3d at 257 (quoting *Roommates.Com*, 521 F.3d at 1167–68). To the extent the

---

company reports "glib statements" purporting to summarize a person's criminal history—"possession of paraphernalia," for example, or "possession-marijuana"—that appear nowhere in the records the company buys. JA30. For named plaintiff Robert McBride, it reported criminal convictions he did not have. JA37–38. In other words, Public Data does not only create its own reports; it creates its own facts.

claims here can be understood to be based on Public Data's content at all, it is Public Data that rendered that content illegal. It is not illegal for the Florida DMV to collect data, or the Maryland Administrative Office of the Courts to have court records. But it is illegal for a company to aggregate that data into a consumer report and sell it to an employer without notifying the subject of the report or requiring the employer to certify they have permission to procure it. Public Data not only "materially contribut[es]" to the alleged illegality here; it is the sole source of that illegality. That alone is sufficient to render Section 230 immunity inapplicable.

4. Finally, even if Public Data neither created nor developed its content, it *still* would not be immune from the plaintiffs' claims here because the "information" it publishes is not "provided by another information content provider" within the meaning of Section 230. The district court assumed that any information an internet company acquires from a third party is "provided by another information content provider"—regardless of whether that third party intended the internet company to post that information online. But, as courts have already recognized, that can't be right. *See, e.g.*, *Roommates.Com*, 521 F.3d at 1171; *Batzel v. Smith*, 333 F.3d 1018, 1032–33 (9th Cir. 2003); *Elliott v. Donegan*, 469 F. Supp. 3d 40, 58 (E.D.N.Y. 2020). That would mean that "users and providers of interactive computer services could with impunity intentionally post material they knew was never meant to be put on the Internet." *Batzel*, 333 F.3d at 1033. And, "[a]t the same time, the creator or developer" of that

material also "presumably could not be held liable" because they did not intend for it to be posted in the first place. *Id.* "The result would be nearly limitless immunity for speech never meant to be broadcast over the Internet." *Id.*

Consider some common-sense examples. Section 230 protects both providers *and users* of interactive computer services from liability for information "provided by another information content provider." 47 U.S.C. § 230(c)(1). If "provided by another information content provider" meant only that the person or company that posted the information online got it from someone else, a surgeon who acquires medical records from their patients' primary care physicians, and then posts those records on a public website, would be immune from civil liability for doing so. A person who gets a letter in the mail from a friend saying that John Smith is a murderer would be immune from liability for posting "John Smith is a murderer" on Facebook—even if they knew it was untrue, and even if the person who sent the letter never meant for it to be posted online. A university that posts all its students' private educational records online would be subject to liability for the records of students who began their education at that university, but not for transfer students' records—as those records would have been acquired from the students' original school. That makes no sense.

Fortunately, Section 230 does not require these absurd results. The district court assumed the phrase "information provided by another information content

provider" refers to information provided *to the internet company* that posted it. But the most natural reading of this phrase is that it refers to information provided *to the internet user*. After all, the whole point of Section 230 is to govern liability for information provided to internet users.[8]

This understanding accords with the ordinary usage of the words "provided by." The ordinary meaning of that phrase is "made available by." *See, e.g.*, Provide, *Webster's New World Dictionary* 474 (1995) (defining "provide" as "to make available"). If a law firm buys snacks for its clients, nobody would say that Nabisco provided the clients snacks; they would say the snacks were made available by—provided by—the law firm. If, on the other hand, Nabisco ran a promotion whereby it gave free cookies to law firms and asked those firms to give the cookies to their clients, then we'd say the cookies were provided by Nabisco. Or, to take another example, if a whistleblower posts their employer's confidential documents online, no online reader

[8] That's also how the word "provided" is used in the definition of information content provider. *Cf. Hall v. United States*, 566 U.S. 506, 519 (2012) ("[I]dentical words and phrases within the same statute should normally be given the same meaning."). Again, an information content provider is an "entity that is responsible . . . for the creation or development of information provided through the Internet . . . ." 47 U.S.C. § 230(f)(3). This definition has to refer to information provided to *users* through the Internet, not information provided to the internet company that posted the information. Otherwise, a person who emailed an internet company information to be posted online would be an information content provider. But a person who mailed the same information with the same request that it be put online would not—they would not have provided the information to the internet company "through the Internet."

would say the documents were made available by the employer. They were provided by the whistleblower—even though they were given to the whistleblower by their employer. But if the employer asked the employee to post the documents, then we'd say they were provided by the employer.

Adopting this more natural reading avoids the absurd conclusion that Section 230 immunizes an internet company for disseminating information online it knows was not intended for dissemination—even information that's illegal to disseminate—just because it got that information from someone else. If someone gives an internet company information for the purpose of putting that information online—by, for example, writing a comment on Facebook or uploading a video to YouTube—then they have made that information available to the company's online users; that information, therefore, has been "provided by another information content provider." But if an internet company decides for itself to put information online, it is the internet company itself that has made the information available to its users—even if it happened to acquire the information from a third party. *See Roommates.Com*, 521 F.3d at 1171. It is, therefore, the internet company itself—and not another information content provider—that has "provided" the information. *See id.*

This understanding of the phrase "provided by" also best effectuates the purpose of Section 230. Congress's goal in passing Section 230 was to incentivize "providers and users of interactive computer services to remove offensive material,

especially obscene and defamatory speech." *Batzel*, 333 F.3d at 1034. Protecting people and companies from liability for internet content, so long as they got it somewhere else, would undermine this goal. *See id.* "[I]mmunizing a publisher or distributor for including content not intended for Internet publication increases the likelihood that obscene and defamatory material will be widely available." *Id.* And not only would this interpretation of Section 230 increase offensive—and illegal—online content, it would chill offline speech. People would be much more hesitant to provide information to others if it could be posted online without their consent—and without any consequences to the poster if they violated the law. *See id.*

The only company that made Public Data's background checks available to its users is Public Data. There's no evidence that any of the companies or government agencies from which Public Data acquires records gave Public Data the records for the purpose of posting them on its website. To the contrary, in many cases the records Public Data buys are expressly *not* intended to be posted online. *See, e.g.*, JA26. For example, federal law requires states to protect the privacy of personal information contained in DMV records. *See* 18 U.S.C. § 2721. So DMVs cannot sell companies personal information to be posted online. Nevertheless, Public Data purchases records from the Florida DMV. JA26. And when it does so, it certifies that the data is for its own use to verify the accuracy of personal information submitted to it. *Id.* But that certification is false. *Id.* Public Data uses the records to create its

reports. *See id.* Therefore, even if Public Data posted these records online verbatim (which it does not), they still could not be said to have been "provided by another information content provider." Without Public Data purchasing them—and lying about why it did so—they would not be available. The records were made available to—that is, "provided" to—Public Data's customers by Public Data.[9]

The reports Public Data creates using these records, therefore, were not "provided by another content provider." They were provided by Public Data.

III. Adopting the district court's flawed interpretation of Section 230 would create a lawless no-man's-land on the internet.

Courts have repeatedly held that companies like Public Data are not above the law just because they operate online. In *Accusearch*, for example, the Tenth Circuit held that a company that bought and illegally sold phone records was not immune from liability under Section 230 simply because it sold those records over the internet. *Accusearch*, 570 F.3d at 1201. In *Brooks v. Thomson Reuters*, the Northern District of California held that a company that aggregates data it procures from third parties into "dossiers of [Californians'] personal information" is not immune from liability

[9] Not only do the entities from which Public Data acquires records not intend to provide them to internet users, many of them are likely not information content providers at all. For example, before the district court, Public Data asserted that it procured records from the Maryland Administrative Office of the Courts. Dkt. 64 at 16. The Administrative Office of the Courts, however, does not "creat[e] or develop[ ]" records, as would be required for it to be an information content provider, 47 U.S.C. § 230(f)(3); it simply stores them. Dkt 68, at 22.

for claims that those dossiers violate the law—even though it sells them online. *Brooks*, 2021 WL 3621837, at *13 (N.D. Cal. Aug. 16, 2021). "These companies"—companies that procure data, aggregate it, and sell it—are "nothing like the paradigm of an" internet company that permits its users to post their own content. *Id.* Their whole purpose is to sell content in violation of the law. They just happen to do it online.

Section 230 "was not meant to create a lawless no-man's-land on the Internet." *Roommates.Com*, 521 F.3d at 1164. If Congress wanted to create a sweeping exemption to the Fair Credit Reporting Act for companies that operate online, it would have said so. *See Morton v. Mancari*, 417 U.S. 535, 551 (1974). But, of course, it didn't. It didn't need to. The Fair Credit Reporting Act poses no threat to the purpose Congress sought to serve in passing Section 230. Companies that serve merely as conduits for others' speech are no less protected from liability if companies that sell employers background checks are required to notify the subject of the background check or provide consumers a copy of their file upon request or adopt reasonable procedures in compiling consumer reports. *Cf. id.* ("The courts are not at liberty to pick and choose among congressional enactments, and when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective.").

Public Data creates background check reports, and sells them in violation of the Fair Credit Reporting Act. Nothing in Section 230 permits it to escape liability

for its illegal conduct, just because it occurs online. This Court should reverse the district court's decision holding otherwise.

CONCLUSION

The district court's judgment should be reversed.

Dated: October 8, 2021

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
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 9,931 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 October 8, 2021, I electronically filed the foregoing brief of plaintiffs-appellees 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