Statement of Jennifer Bennett
Principal, Gupta Wessler PLLC, San Francisco, CA

Before the United States Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

"Platform Accountability: *Gonzalez* and Reform"

March 8, 2023

Chair Blumenthal, Ranking Member Hawley, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today. I am a principal at Gupta Wessler PLLC, a law firm focused on Supreme Court and appellate advocacy in the public interest. I have appeared before trial and appellate courts across the country, both state and federal, as well as the U.S. Supreme Court on behalf of workers, consumers, and civil-rights plaintiffs.

Although the title of this hearing references *Gonzalez v. Google*, I've been invited here today to discuss another Section 230 case: *Henderson v. Public Data*, an appeal that I recently argued before the Fourth Circuit. And the reason that case is interesting is because the one thing all of the litigants in *Gonzalez* seemed to agree on is that the decision in that case is correct.[1] So in thinking about what Section 230 means and how it might clarified, *Henderson* is a useful starting point.

I will explain the court's decision in more detail. But the bottom line is that *Henderson* focuses on a key distinction—and this is the distinction I think everyone is agreeing with when they say *Henderson* is correct. That key distinction is between liability based solely on the content that a platform's users have posted—the core of what Section 230 is designed to protect against—and liability based on the platform's *own* conduct, which Section 230 does not shield.

Background. Before diving into the decision, a bit of background on the case: The defendant in *Henderson* is Public Data, an online background check company. As alleged in the complaint, the company buys personal data about people across the country—including criminal records, court records, and DMV records—much of which is governed by laws restricting its distribution. And it uses this data to compile

---

[1] *See* Oral Arg. Tr. 3 (petitioners' counsel stating that "*Henderson* correctly interprets the statute"); *id.* at 144 (respondent's counsel stating that *Henderson*'s "test is correct"); United States Br. 16 (discussing *Henderson* with approval). The oral argument transcript is available at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2022/21-1333_p8k0.pdf. The Government's amicus brief is available at https://www.supremecourt.gov/DocketPDF/21/21-1333/249441/20221207203557042_21-1333tsacUnitedStates.pdf.

its own "original, proprietary" background check reports, which it then sells online to employers, landlords, and lenders.[2]

In creating these reports, Public Data does not merely regurgitate the 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. Public Data's customers then use these reports to make crucial decisions on everything from hiring to renting to creditworthiness.

Background screening, like that provided by Public Data, is a multi-billion-dollar industry. Over ninety percent of employers and landlords use background checks to evaluate prospective tenants and employees. So a background-check error—a false criminal conviction, for example—can make it impossible to find work or housing. 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 people 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.[3]

But Public Data has chosen not to comply with the Fair Credit Reporting Act. The *Henderson* case arose out of this choice. The lawsuit was brought by Tyrone Henderson, George Harrison, and Robert McBride, Virginians who have lost housing or employment opportunities because of inaccurate information reported about them in their background checks. Background checks on Mr. Henderson, for example, often report that he has a felony history that is not, in fact, his, but rather that of another person with a similar name. Public Data's background check for Mr. McBride listed multiple criminal offenses, for which he was never actually prosecuted.

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. Although the Fair Credit Reporting Act requires consumer reporting agencies to provide consumers' files upon request, Public Data refused. 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. And Public Data does not require that employers certify

[2] Unless otherwise specified, all of the factual allegations and quotations in this section are drawn from the second amended complaint in *Henderson*, which is available at Docket No. 56, Case No. 20-294 (E.D. Va.).

[3] *See* 15 U.S.C. §§ 1681g, 1681k(a), 1681b(b)(1), 1681e(b).

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.

Mr. Henderson, Mr. Harrison, and Mr. McBride, therefore, sued Public Data for its violations of the Fair Credit Reporting Act. In response, Public Data argued that because it operates online, Section 230 immunizes it from claims brought under the statute. Its argument was opposed by a broad, diverse coalition of *amici* including the State of Texas, as well as twenty other states, the Consumer Financial Protection Bureau and the Federal Trade Commission, consumer protection groups, workers' rights groups, and civil rights groups.

The Fourth Circuit rejected the contention that Section 230 immunizes Public Data from Fair Credit Reporting Act claims, simply because the company operates online. Section 230 provides that: "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."[4] By its terms, the Fourth Circuit explained, the statute only shields online companies from claims that (1) treat them as the publisher of (2) content "provided by another information content provider." The claims in *Henderson*, the court held, didn't satisfy these requirements. Section 230, therefore, did not shield Public Data from liability. And in explaining why, the court gave voice to what seems to be a growing consensus view about what Section 230 means.[5]

"Treated as the publisher." The *Henderson* court started by considering what it means for a claim to treat an internet company as a publisher. The court explained that "the term publisher as used in § 230(c)(1) derives its legal significance from the context of defamation law." That's because the purpose of Section 230 was to overrule *Stratton Oakmont*, a defamation case that had imposed liability on an internet platform for its users' postings, simply because the platform had made an effort to take down offensive posts. That effort, *Stratton Oakmont* held, rendered the platform a publisher liable for its users' speech. The point of Section 230 is to prevent this kind of liability. So when the statute bars claims that treat an internet company as a publisher, it's referring to claims that impose publisher liability as that term was understood in common law defamation claims—like the claims in *Stratton Oakmont*.

[4] 47 U.S.C. § 230(c)(1).

[5] The Fourth Circuit's opinion is available at *Henderson v. Source for Pub. Data, L.P.*, 53 F.4th 110 (4th Cir. 2022). Unless otherwise specified, all internal quotation marks, citations, and alterations are omitted from quotations of the case, as well as other quotations in this statement.

The Fourth Circuit in *Henderson* explained that at common law, publisher liability had two requirements. First, a publisher was someone who disseminated information to third parties. But information dissemination "was not enough." There was a second requirement for publisher liability: improper content. "[T]o hold someone liable as a publisher at common law was to hold them responsible for the . . . improper character" of the content they published.

Thus, the court held, "a claim only treats" an online platform as a publisher under Section 230, "if it (1) bases the defendant's liability on the disseminating of information to third parties and (2) imposes liability based on the information's improper content." Based on this plain-text, historical reading of Section 230, the court rejected the argument that Section 230 immunizes platforms from any claim that "hinges in any way on the act of publishing"—or, put in legal terms, any claim in which "publication [is] a but-for cause of the [plaintiff's] harm." That's not what publisher liability meant when Section 230 was enacted—and so it's not what Section 230 means when it prohibits treating a platform as a publisher.

Applying this understanding to the claims in *Henderson*, the court held that Section 230 "does not provide blanket protection" from all Fair Credit Reporting Act claims simply because the Act only applies to companies that publish credit information. The relevant question is—with respect to "each specific claim"—whether that claim (1) holds someone liable for disseminating information to third parties (2) based on that information's improper content.

The court's application of that test to the claims in *Henderson* is instructive. The plaintiffs' claim that Public Data failed to provide them a copy of their file, the court held, did not treat the company as a publisher because it failed prong 1 of the publisher liability test: dissemination to a third party. The claim was based on Public Data's failure to disseminate information to the subject of that information—not someone else. The plaintiffs' claim that Public Data unlawfully sold background checks without requiring purchasers to certify they had permission and a proper purpose, the court held, failed prong 2 of the publisher liability test: improper content. The claim didn't depend in any way on the propriety of the data Public Data published; it was based solely on Public Data's failure to obtain the proper certifications before doing so. On the other hand, the court suggested that any claims that sought to hold an online company liable because the background checks it sold were inaccurate, could potentially be understood as treating the company as a publisher within the meaning of Section 230.[6] That's because those claims would seek to impose liability for disseminating improper content to third parties.

[6] The court did not actually decide the issue.

Put simply, *Henderson* draws a clear line between imposing liability because a platform disseminates unlawful content and imposing liability for the platform's conduct. Only the former treats the platform as a publisher.

"Provided by another information content provider." But, as *Henderson* explains, Section 230 does not immunize online companies even from all claims that treat them as a publisher. It protects platforms only from those claims that would treat them as "the publisher" of "information provided by *another* information content provider."[7] In turn, the statute defines "information content provider" as someone "responsible, in whole or in part, for the creation or development of information provided through the Internet."[8] Courts agree, therefore, that Section 230 does not immunize companies for any content that they themselves are "responsible" for creating or developing, even "in part."

Here, too, *Henderson*'s analysis is informative. *Henderson* explains the widespread agreement among courts that, at the very least, a platform "develop[s]" content—and therefore falls outside of Section 230's protection—when its "own actions contribute[ ] in a material way" to what makes the content improper. Thus, the court held that Section 230 did not shield Public Data from claims that, in publishing data it collected from others, the company "omitted or summarized information in a way that made it misleading." Doing so, the court explained, goes beyond the kind of "formatting" or "procedural alterations" necessary to enable a platform to publish third-party content and makes the platform itself responsible—at least in part—for the content.

This line accords with the purpose of Section 230. The statute "prevents suits that cast [an online platform] in the same position as the party who originally posted the offensive messages." That is, it prevents lawsuits that merely seek to impose "vicarious liability" on a platform for its users' speech. But it does not shield online companies "when the offensiveness" of the content stems from the platform itself.

Growing consensus. *Henderson* does not stand alone. There is a growing consensus that Section 230 does not—and was never intended to—shield a platform from liability for its own conduct.[9] Take, for example, the Ninth Circuit's decision in *Lemmon v. Snap.* In that case, the parents of two teenagers who died in a car accident sued Snap, a social media company, alleging that the accident was caused by Snap's negligent design of its cellphone app, SnapChat. According to the parents, SnapChat incentivizes users to send videos and photos (called "snaps") to other

---

[7] 47 U.S.C. § 230(c)(1) (emphasis added).

[8] *Id.* § 230(f)(3).

[9] *See, e.g.*, *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021); *Fed. Trade Comm'n v. LeadClick Media, LLC*, 838 F.3d 158 (2d Cir. 2016); *F.T.C. v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc); *Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021).

users on the platform by rewarding them based on the snaps they send. SnapChat also offers users a "Speed Filter," which allows them to capture how fast they are going and overlay that information onto a video or photo. The parents alleged that SnapChat knew that its users believed the app would reward them for recording a snap at 100 miles per hour or faster and sharing it on the platform, and thus that it was leading young drivers to drive dangerously fast. In fact, there had been a series of news articles about the danger, other accidents, and even a previous lawsuit. In other words, the parents alleged that Snap designed an application that incentivized dangerous driving, knew that the app was causing accidents, and yet refused to do anything about it.[10]

In response, Snap argued that Section 230 protected it from liability. The Ninth Circuit rejected the argument for similar reasons that *Henderson* rejected Public Data's Section 230 argument. *First*, the court held that the parents' negligent-design claim didn't treat Snap as a publisher. It didn't seek to hold the company liable for improper content; it sought to hold the company liable for designing a dangerous product. "The duty to design a reasonably safe product is fully independent of Snap's role in monitoring or publishing third-party content." *Second*, the court held that the parents' claim didn't seek to hold Snap liable for third-party content. The basis of their claim was Snap's own design choices: its own architecture, its own "Speed Filter," its own rewards system.

Stepping back, the court explained, Snap "is an internet publishing business. Without publishing user content, it would not exist." But just because "publishing content" is a "cause of just about everything" Snap does, that doesn't mean that Section 230 shields Snap from all liability. Section 230 "was not meant to create a lawless no-man's-land on the Internet." It shields platforms from claims against them based on the speech their users publish; it does not immunize companies for their "own acts."

Conclusion. The litigants in *Gonzalez v. Google* disagree about virtually everything except that *Henderson* provides the correct framework for analyzing claims of immunity under Section 230. As this subcommittee, and Congress more generally, considers Section 230, *Henderson* provides a blueprint for what Section 230 was always meant to be: a shield from liability based on internet users' content, not platforms' own conduct.

* * *

Thank you again for the opportunity to testify today. I look forward to your questions.

[10] The Ninth Circuit's decision is available at *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021).