No. 22-16993

In the United States Court of Appeals for the Ninth Circuit

PATRICK CALHOUN; ELAINE CRESPO; MICHAEL HENRY; CORNICE WILSON; RODNEY JOHNSON; CLAUDIA KINDLER,
Plaintiffs-Appellants,

v.

GOOGLE, LLC,
Defendant-Appellee.

On Appeal from the United States District Court
for the Northern District of California, Oakland Division

BRIEF FOR THE STATE OF TEXAS AND 18 OTHER STATES AS AMICI CURIAE IN SUPPORT OF APPELLANTS

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

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

AARON L. NIELSON
Solicitor General

LANORA C. PETTIT
Principal Deputy Solicitor General
Lanora.Pettit@oag.texas.gov

BILL DAVIS
Deputy Solicitor General

KYLE D. HIGHFUL
Assistant Solicitor General

Counsel for Amici Curiae

[Additional counsel listed at end of brief]

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes and Rules:

Other Authorities:

Statement of Interest of Amici Curiae

Google products, including the Chrome web browser, are ubiquitous in the lives of Amici States' citizens. Indeed, Google is so omnipresent that it has become a verb, defined as "us[ing] the Google search engine to obtain information about (as a person) on the World Wide Web." *Merriam-Websters Collegiate Dictionary*, 539 (11th ed. 2003). Amici States have an interest in making sure that Google is held accountable when it abuses their citizens' trust—an interest which has led every State to pursue Google for its deceptive trade practices in collecting data.[1] Amici States have a further interest in courts construing online agreements in favor of ordinary consumers rather than the giant tech companies that draft the agreements while holding the keys to the internet—a tool upon which many Americans depend every day for work, education, entertainment, and social interaction. Because the plaintiffs here allege that

[1] *E.g.*, Dave Collins & Marcy Gordon, *40 States Settle Google Location-Tracking Charges for $392M*, AP News (Nov. 14, 2022), https://apnews.com/article/google-privacy-settlement-location-data-57da4f0d3ae5d69b14f4b284dd084cca (all cited websites last accessed Dec. 18, 2023); Angela Cordoba Perez & Jose R. Gonzalez, *Google to Pay Arizona $85M in Privacy Suit that Alleged 'Deceptive' Location Tracking*, USA Today (Oct. 5, 2022, 11:28 a.m.), https://www.usatoday.com/story/money/2022/10/05/google-arizona-lawsuit-settlment-85-million/8185226001; Jared Gans, *Google to Pay $29.5 Million to Settle DC, Indiana Lawsuits Over Location Tracking*, The Hill (Dec. 31, 2022), https://thehill.com/policy/technology/3794301-google-to-pay-29-5-million-to-settle-dc-indiana-lawsuits-over-location-tracking; Jonathan Stempel, *Google Reaches $39.9 Million Privacy Settlement with Washington State*, Reuters (May 19, 2023, 9:33 a.m.), https://www.reuters.com/legal/google-pay-399-mln-washington-state-over-location-tracking-practices-2023-05-18.

Google violated its agreements and stole their personal information for profit, this case implicates those state interests.[2]

INTRODUCTION

Google, a subsidiary of Alphabet, Inc., "dominates the Internet." Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 Utah L. Rev. 1433, 1434 (2008). Starting as a small search engine, Google has developed an integrated suite of software, internet-based, and hardware products, that allow Google users to access Google-run networks through Google-created applications on Google-branded smartphones. These loyal users, however, are not Google's primary customers. That distinction goes to online advertisers who pay Google to assist them to target their messages to users most likely to buy their products. Megan Graham & Jennifer Elias, *How Google's $150 Billion Advertising Business Works*, CNBC (Oct. 13, 2021, 12:52 p.m.), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html (describing how Google has been "the market leader in online advertising for well over a decade").

"Google's business model is based on trust." *In re Alphabet, Inc. Sec. Litig.*, 1 F.4th 687, 704 (9th Cir. 2021), *cert. denied sub nom. Alphabet Inc. v. Rhode Island*, 142 S. Ct. 1227 (2022). The plaintiffs in this case allege that Google violated that trust. *Calhoun v. Google, LLC*, 645 F. Supp. 3d 916, 920–21 (N.D. Cal. 2022) ("*Calhoun II*"). Plaintiffs allege that they chose not to sync their Chrome web browsers to

[2] Amici States are authorized to file this brief under Federal Rule of Appellate Procedure 29(a)(2). No party or counsel assisted in or paid for the preparation of this brief.

a Google account and understood based on Google's own privacy agreements that this would give them control over their personal information.[3] But Google collected their personal information anyway and claimed consent. The district court agreed and granted summary judgment for Google. The court reached that conclusion only after neglecting the reasonable-user standard, collating multiple agreements, and considering technical evidence provided by experts that would have been unavailable to the users whose information was surreptitiously gathered. That was error, and this Court should reverse.

SUMMARY OF THE ARGUMENT

I. Google is no stranger to litigation. Given the risks created by its business model, which incentivizes maximum data collection, it is unsurprising that numerous plaintiffs—including all 50 States and the District of Columbia, *supra* n.1—have alleged that Google violated the privacy of its users. Notwithstanding its extensive physical presence in other States, Google has repeatedly asserted that any such suit must be brought in the Northern District of California. Although such demands are meritless and have met with far from universal success, the precedent that the Court sets in this case should be assumed to affect consumer protection on a much larger scale.

---

[3] For a discussion of how Google's privacy terms have evolved and expanded over "two decades and 30 versions," *see* Charlie Warzel & Ash Ngu, *Google's 4,000-Word Privacy Policy Is a Secret History of the Internet*, NYTimes (July 10, 2019), https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html.

II. The district court erred in granting Google's motion for summary judgment by viewing Google's privacy agreements through the lens of a sophisticated party with technical expertise and access to detailed information about the inner workings of Chrome and other web browsers. This mode of analysis erroneously departs from other decisions that have viewed online privacy agreements from the perspective of a reasonable *user*, who has little ability to completely avoid Google products and thus little choice but to accept Google's boilerplate terms. A reasonable user could have read the Chrome Privacy Notice and concluded that it meant what it said: Chrome would not send the user's personal information to Google unless the user synced Chrome with a Google account. Even if the Court concludes that the privacy agreements were ambiguous, Google has hardly met its burden to obtain summary judgment on the grounds of consent, either because ambiguity is construed against the drafter or because consent must be unambiguous.

ARGUMENT

I. This Case Fits Into a Larger Pattern of Google Allegedly Violating Its Users' Trust.

"Search engines are the central actors on the Internet today and Google is the undisputed king of search." Tene, *supra*, at 1434. As far back as 2008, Google was "estimated to account for nearly 60% of all Internet search queries in the United States—over six billion each month." *Id.* at 1434 n.3. Today, the strength of Google's advertising platform has propelled its parent company, Alphabet, into being the world's seventh largest company—behind only Saudi Aramco and five of the world's largest banks. Andrea Murphy & Hank Tucker, *The Global 2000*, Forbes

(June 8, 2023), https://www.forbes.com/lists/global2000/?sh=e9de10b5ac04. It received more revenue in 2022 than the State of Texas. *Compare Profile: Alphabet*, Forbes, https://www.forbes.com/companies/alphabet/?list=global2000&sh=1154864b540e (listing $257.5 billion), *with* Tex. Comptroller of Pub. Accts., *Texas Comptroller Glenn Hegar Announces Revenue for Fiscal 2022, August State Sales Tax Collections* (Sept. 1, 2022), https://tinyurl.com/54dkvcye ($183.34 billion).

Because Google's internet users do not pay to search, it has obtained its dominant position in the digital marketplace only because "[e]very day, millions of users provide Google with unfettered access to their interests, needs, desires, fears, pleasures, and intentions." Tene, *supra*, at 1435. Indeed, Google has become "a central database" for users' "entire digital lives." *Id.* And Google's business model centers on the monetization of users' data through targeted advertising. *See Jones v. Google LLC*, 73 F.4th 636, 640 (9th Cir. 2023); *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 973–74 (N.D. Cal. 2014); Graham & Elias, *supra*.

Google's "access to and storage of vast amounts of personal information" has created what is "perhaps the most difficult privacy [problem] in all of human history." Tene, *supra*, at 1435 (alteration in original). Google has every incentive "not only to collect as much user data as possible, but also to keep it for a long period of time." Kathleen E. Kubis, *Google Books: Page by Page, Click by Click, Users Are Reading Away Privacy Rights*, 13 Vand. J. Ent. & Tech. L. 217, 227 (2010). Even Google has acknowledged its responsibility as the custodian of so much personal information: "When you use our services, you're trusting us with your information. We

understand this is a big responsibility . . . ." Google, *Privacy Policy*, https://policies.google.com/privacy.

Although Google has so far maintained its monopolistic grip on key internet services, it is now plagued by allegations that it has abused its access to nearly every aspect of its users' personal lives. Amid the myriad lawsuits against Google is one brought by the State of Texas alleging that Google violated the State's Deceptive Trade Practices–Consumer Protection Act. Amended Br. for Appellee at 12, *Google LLC v. State*, No. 13-23-00114-CV (Tex. App.—Corpus Christi–Edinburg Aug. 23, 2023). Specifically, Texas alleges that Google deceives users regarding their ability to control how Google tracks their locations. *Id.* at 13–14. Texas further alleges that Google continues to collect data regarding a user's search history even when that user enables Incognito Mode and other privacy settings that Google has advertised as allowing Texans to control what data Google collects, sends, and stores. *Id.* at 14. Nor is Texas alone in challenging Google's "surreptitious interception and collection of personal and sensitive user data while users are in 'private browsing mode.'" *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *1 (N.D. Cal. Aug. 7, 2023); *see In re Google Inc. St. View Elec. Commc'ns Litig.*, 21 F.4th 1102, 1107 (9th Cir. 2021) ("[P]laintiffs alleged, on behalf of an estimated sixty million people, that Google illegally collected their Wi-Fi data through its Street View program."), *cert. denied sub nom. Lowery v. Joffe*, 143 S. Ct. 107 (2022).

Thus, this case represents just one front in a larger conflict in which federal and state governments, along with private plaintiffs, are fighting to rein in alleged abuses by tech giants like Google, and the Court's decision here may have repercussions

well beyond this case. That is particularly so because Google has repeatedly insisted that any litigation about its terms of service must be brought in the Northern District of California based on some combination of the location of its corporate headquarters and a forum-selection clause that Google slipped into its terms of service—to which users have little choice but to agree if they are going to be able to function in a Google-dominated world. *See, e.g.*, Appellant's Br. at 44–46, *Google LLC v. Texas*, No. 13-23-00114-CV (Tex. App.—Corpus Christi–Edinburg June 12, 2023). Because such arguments are often irreconcilable with jurisdictional, venue, or contract-interpretation rules in most States, they have been far from universally successful—particularly when a State or other governmental entity is the plaintiff. *E.g.*, Order, *District of Columbia v. Google*, No. 2002 CA 000330 B (D.C. Sup. Ct. Aug. 31, 2022) (refusing to dismiss a case based on personal-jurisdiction arguments); *State v. Google LLC*, No. 22-2-01103-3 SEA (Wash. Sup. Ct. King Cnty. May 20, 2022); *see* Marty Gould, *The Conflict Between Forum-Selection Clauses and State Consumer Protection Laws: Why Illinois Got It Right in* Jane Doe v. Match.com, 90 Chi.-Kent L. Rev. 671, 686 (2015). Nevertheless, this Court's rule will apply to a disproportionate number of suits aimed at holding Google to the promises it has made its users.

II. The District Court Erred in Granting Google's Motion for Summary Judgment.

This Court should hold that the district court improperly construed Google's privacy agreements collectively and in the light of expert testimony. Instead, the court should have asked whether a user could have *reasonably* believed that Google would collect personal information even when the user chose not to sync Chrome

with a specific account. After all, a reasonable user could have understood browsing in *Chrome* to be governed by the *Chrome* Privacy Notice—not miscellaneous documents that even the district court claimed to understand only after holding an evidentiary hearing. The Chrome Privacy Notice specified that a user "[doesn't] need to provide any personal information to use Chrome." *Calhoun II*, 645 F. Supp. 3d at 924 (emphasis omitted). And any ambiguity on this point should have worked in Plaintiffs' favor, not Google's. Accordingly, the district court should have denied Google's motion for summary judgment on consent.

A. The district court should have determined how a reasonable user—not an expert—would understand the privacy agreements.

Google's motion for summary judgment argued that Plaintiffs' claims were barred because Plaintiffs "consented to Google's receipt and use of the at-issue data." *Id.* at 928. To determine whether Plaintiffs had consented, however, the district court considered not just Chrome's Privacy Notice, but four additional documents as well: (1) Google's General Terms of Use, (2) Google's General Privacy Policy; (3) a Consent Bump Agreement "that Google showed to account holders either when they visited a Google owned-and-operated property while signed into their account or when users signed into their account for the first time after June 2016" (quotation marks omitted); and (4) New Account Creation Agreement. *Id.* at 922–27. Each of Google's privacy disclosures is thousands of words long. Warzel & Ngu, *supra*. Indeed, just the parts of those agreements that the district court considered relevant spanned multiple pages, *Calhoun II*, 645 F. Supp. 3d at 922–27, and speak in technical terms like "Internet protocol address," *id.* at 923, "device event

information," *id.*, and "first-party cookies," *id.*, which would have been incomprehensible to most Google users.

In addition, the district court compounded its error when, "[t]o better understand the parties' positions, and to have a more fulsome record," it held an evidentiary hearing to determine what users may have consented to. *Id.* at 929. "The hearing lasted approximately 7.5 hours and included live testimony from eight witnesses," including experts. *Id.* Those experts did not testify about how the average Google user might understand the complex documents associated with Google products but instead went even deeper into the minutiae of internet technologies, treating such topics as whether "the X-client-data identifier" was "browser-agnostic," *id.*, and whether the "GET and POST communications" used by other browsers are "as detailed and specific as the information in the Chrome browser," *id.* at 931.

Although the district court's desire to understand the issues presented in this case is laudable, this technical analysis took the court far afield from its proper inquiry. As the court itself briefly acknowledged, it needed to decide how "a reasonable person" would understand Google's disclosures. *Id.* at 935. But a reasonable person trying to access local services or look up the location of a doctor is not an expert with leisure to study each of the documents, compare them line by line, and then apply technical knowledge about how various browsers function.

This analysis is at odds with other cases from the Northern District of California. For example, *In re Meta Pixel Healthcare Litigation* involved the "alleged use of proprietary computer code to obtain certain healthcare-related information of Facebook users." No. 22-CV-03580-WHO, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22,

2022). A "key question" in the case was whether the plaintiffs had consented to the defendant's acquisition of their health information. *Id.* at *8. As the court explained, "[t]he test is whether a *reasonable user* who viewed Meta's disclosures would have understood that Meta was collecting the information at issue." *Id.* at *9 (emphasis added). The court noted that "Meta's policies notify Facebook users that Meta collects and uses their personal data, including data about their browsing behavior on some third-party websites, at least in part for targeted advertising." *Id.* But it concluded that "Meta's policies do not, however, specifically indicate that Meta may acquire *health data* obtained from Facebook users' interactions with their *medical providers' websites*. Its generalized notice is not sufficient to establish consent." *Id.* And the court further noted that, for consent to be effective, "Meta's policies 'must have only one plausible interpretation.'" *Id.* at *10 (quoting *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) ("*Calhoun I*")). Accordingly, the court "d[id] not believe that a reasonable user would have understood that Meta may intercept their health information." *Id.* at *8.

More recently, in *Brown*, the plaintiffs "challenge[d] Google's alleged collection of their data while they were in private browsing mode." *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1055 (N.D. Cal. 2021). Google argued that the plaintiffs had consented to the data collection. *Id.* at 1062–63. The court explained that "[i]f a reasonable . . . user could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct, then [the defendant] cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)." *Id.* at 1063 (quoting *In re Facebook, Inc., Consumer Privacy User Profile Litig.*,

402 F. Supp. 3d 767, 789–90 (N.D. Cal. 2019)). Because Google never *specifically* informed the plaintiffs that it would collect information during private browsing—even though the Privacy Policy stated generally that Google collects information—the court rejected Google's argument that the plaintiffs had consented. *Id.* at 1064. As the court explained, "a Google user reading the general disclosure above, which never mentions private browsing mode, might have reasonably concluded that Google does not collect this data from users in private browsing mode." *Id.* That was particularly true because, when a user entered into private browsing, an "Incognito Splash Screen" was displayed declaring that the user could "browse privately." *Id.* at 1064–65.

Indeed, the district court's summary judgment order is inconsistent with its own analysis of the correct standard during an earlier phase *of this very case*. When Google moved to dismiss under Rule 12(b)(6), Judge Koh held that Google had not shown that Plaintiffs consented to Google's receipt of their data. *Calhoun I*, 526 F. Supp. 3d at 619–23. She acknowledged that Google's General Privacy Policy disclosed the collection of information. *Id.* at 620–21. But she determined that this general disclosure was insufficient, given that "the Chrome Privacy Notice makes specific representations that could suggest to a reasonable user that Google would not engage in the alleged data collection." *Id.* at 621. That was the right methodology and the right result.

Although not binding on this Court, these decisions were correct to apply the reasonable-user approach rather than the expert-analyst approach adopted by the district court. Under ordinary interpretive rules, contracts involving a member of the

general public are typically construed from the perspective of a layman of average intelligence. Courts have applied that rule in the insurance context, for example. *See, e.g.*, *Zhao v. CIEE Inc.*, 3 F.4th 1, 7 (1st Cir. 2021) (discussing Maine law); *Telamon Corp. v. Charter Oak Fire Ins. Co.*, 850 F.3d 866, 869 (7th Cir. 2017) (discussing Indiana law); *Hyman v. Nationwide Mut. Fire Ins. Co.*, 304 F.3d 1179, 1190 (11th Cir. 2002) (discussing Florida law); *Lee v. USAA Cas. Ins. Co.*, 22 P.3d 631, 636 (Mont. 2001).

And the Court should apply it here as well. After all, the question is what Google users *consented to* when they used Google products. *Calhoun II*, 645 F. Supp. 3d at 932. The drafter of these privacy agreements is a sophisticated, well-funded corporation with extensive legal and technical expertise, but the average Google user has no access to—or, likely, the ability to understand—the kind of information developed at an evidentiary hearing. Technical information that the user never saw and likely could not comprehend is irrelevant in determining what the user agreed to in accepting Google's terms. *See Calhoun I*, 526 F. Supp. 3d at 620 (noting that "consent must be actual").

In addition, although users are, strictly speaking, free to accept or reject Google's terms, Google's monopoly on key internet services raises the question: "*What if there is no meaningful choice?* What if, that is, consumers, however well informed they may be about a seller's privacy practices, have no meaningful alternative but to subject themselves to a set of privacy practices that they would prefer to avoid?" John A. Rothchild, *Sham Choice: How the Current Privacy Regime Fails Us, and How to Fix It*, 92 UMKC L. Rev. 169, 171 (2023).

The lack of meaningful alternatives has led some courts to hold contracts unenforceable as against public policy. *See, e.g.*, *Tunkl v. Regents of Univ. of Cal.*, 383 P.2d 441, 446–47 (Cal. 1963); *see also Disc. Fabric House of Racine, Inc. v. Wis. Tel. Co.*, 345 N.W.2d 417, 425–26 (Wis. 1984). That is because

> [i]mplicit in the principle of freedom of contract is the concept that at the time of contracting each party has a realistic alternative to acceptance of the terms offered. Where goods and services can only be obtained from one source (or several sources on non-competitive terms) the choices of one who desires to purchase are limited to acceptance of the terms offered or doing without. Depending on the nature of the goods or services and the purchaser's needs, doing without may or may not be a realistic alternative.

Allen v. Mich. Bell Tel. Co., 171 N.W.2d 689, 692 (Mich. Ct. App. 1969).

Recent legislative initiatives across the country reflect that this is an area where, at a minimum, the lack of reasonable alternatives should lead courts to adopt a heightened scrutiny when determining whether an average user has consented to online boilerplate agreements. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, NY Times: Wirecutter (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us (describing the "bunch of disparate federal [and state] laws" regarding data privacy that have been enacted over the last several years) (alteration in original). That is true even assuming courts "pretend that users actually read [a website's] contractual language before clicking their acceptance, even though we all know virtually none of them d[o]." *In re Facebook*, 402 F. Supp. 3d at 789.

A recently enacted Texas law provides an example of how States are acting to help protect consumer data. Act of May 28, 2023, 88th Leg., R.S., ch. 995 (to be

codified at Tex. Bus. & Com. Code ch. 541) ("H.B. 4"). The law provides a definition of "consent" applicable to the consumer-protection context:

> "Consent," when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. The term does not include:
>
> (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;
>
> (B) hovering over, muting, pausing, or closing a given piece of content; or
>
> (C) agreement obtained through the use of dark patterns.

Id. (to be codified at Tex. Bus. & Com. Code § 541.001(6)). A dark pattern is "a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a dark pattern." *Id.* (to be codified at § 541.001(10)).

The definition of consent in Texas's law—which is far from unique—recognizes that privacy policies, even if truthful, can be buried in masses of text, delivered in fleeting pop-ups, or obscured by distracting visuals. It also recognizes that, given the significance of the personal information that users often share online, consent to use that information must be "specific, informed, and unambiguous." *Id.* (to be codified at § 541.001(6)). Here, such consent was entirely lacking—let alone informed and unambiguous.

B. A reasonable user could have concluded that Google would not collect personal information from an un-synced Chrome browser.

The court started in the right place when it noted that although "consent can be express or implied," it "must be actual." *Calhoun II*, 645 F. Supp. 3d at 928 (cleaned up) (quoting *In re Google, Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *12 (N.D. Cal Sept. 26, 2013)). And it correctly explained that "[c]onsent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and if the alleged tortfeasor did not exceed the scope of that consent," *id.* at 928 (quoting Restatement (Second) of Torts § 892A (1979)), which in turn requires that Google's disclosures "'explicitly notify' users of the conduct at issue," *id.* at 929. It skipped a step, however, by failing to note that consent is effective only if the agreement is susceptible to just one plausible interpretation. *Compare Brown*, 525 F. Supp. 3d at 1063, and *Calhoun I*, 526 F. Supp. 3d at 620, *with Calhoun II*, 645 F. Supp. 3d at 928–29. It also failed to mention the reasonable-user standard. *Calhoun II*, 645 F. Supp. 3d at 928–29. This omission caused its analysis to go astray.

The Chrome Privacy Notice purported to allow users to "learn how to control the information that's collected, stored, and shared when [they] use the Google Chrome browser." *Id.* at 924. The notice stated, "**You don't need to provide any personal information to use Chrome,** but Chrome has different modes you can use to change or improve your browsing experience." *Id.* It further explained, "**The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync** . . . ." *Id.* And

although the notice indicated that synced personal information was subject to the more general Privacy Policy, it assured users, "Sync is only enabled if you choose." *Id.* at 925.

Rather than hold Google to the terms of that representation—*i.e.*, that by not syncing Chrome to an account, a user could protect his personal data from intrusion—the court provided a lengthy discussion of the technical matters explored at the evidentiary hearing. *Id.* at 929–31. According to the court, the evidence showed that "the at-issue data, except for the X-client-data identifier, is browser-agnostic." *Id.* at 929. That was significant because, in the court's view, the fact "that the at-issue data collected is not specific to Chrome but browser agnostic" implied "that Google's general policies," rather than the Chrome Privacy Notice, applied to Plaintiffs' browsing. *Id.* at 931.

The court's analysis is questionable even on its own terms. Just because most of the data collected by Chrome would also be collected by other browsers does not mean that the Chrome Privacy Notice would not govern here. After all, whether Safari or Firefox would ordinarily collect the information says nothing about whether Chrome would collect the information when not synced with a user's Google account. And that is particularly true given that the Chrome Privacy Notice assured users, "**You don't need to provide any personal information to use Chrome**" and "**The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync** . . . ." *Id.* at 924.

In any event, the court's analysis is flawed because it was based on information beyond the reach of the average user. The anonymous "reasonable user" is not privy to multi-hour evidentiary hearings and lacks the technical expertise of the parties' witnesses. Such a user would not know what information is browser-agnostic and what is particular to Chrome. Instead, the reasonable user would read the Chrome Privacy Notice, understand that he or she could avoid sending personal browsing information to Google by not syncing an account, and assume that the more specific Chrome Privacy Notice would control over more general agreements. Indeed, a reasonable user would be unlikely to look to *other* disclosures to find out how Google would handle privacy for *Chrome*. In sum, the court should have concluded, as Judge Koh did when evaluating Google's motion to dismiss, that "a reasonable user could read Google's representations to mean that, if the user was not synced, his or her browsing history, cookies, and site data would not be sent to Google." *Calhoun I*, 526 F. Supp. 3d at 622.

The district court tried to explain that it did not follow *Calhoun I* because *Calhoun I* "consider[ed] plausibility" of the allegations in Plaintiffs' complaint, whereas *Calhoun II* was bound by "the actual factual record." *Calhoun II*, 645 F. Supp. 3d at 934 n.8. That explanation, even if accurate, misses the main point. Judge Koh did not just apply a different burden of proof in a different procedural posture: she asked a different legal *question*—and correctly so. Specifically, the court in *Calhoun II* asked whether a sophisticated user with the time and resources to scour all of Google's disclosures and analyze technical data regarding various browsers would conclude otherwise. *Id.* at 921–31. By contrast, *Calhoun I* asked whether a reasonable user of

Chrome would understand the Chrome privacy agreements to mean that Google would not collect personal information from a non-synced Chrome browser. 526 F. Supp. 3d at 619–23. Because Judge Koh got the framework right in *Calhoun I*, the Court should reverse.

C. If the privacy agreements are ambiguous, then Google failed to meet its summary-judgment burden.

Even if the Court concludes that Google's privacy agreements should be read together and that they are ambiguous when so analyzed, it should still reverse the district court's summary judgment for either of two reasons.

First, under the "doctrine known as *contra proferentem*," an ambiguous contract is construed against the drafter. *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1417 (2019). This rule "enjoys a place in every hornbook and treatise on contracts," and is "based on public policy factors, primarily equitable considerations about the parties' relative bargaining strength." *Id.* Those public policy factors weigh heavily in Plaintiffs' favor. The drafter here was Google, which "dominates the Internet." Tene, *supra*, at 1434. And Google's parent company, Alphabet, Inc., is consistently ranked among largest companies in the world. *Supra* p. 4. Plaintiffs, on the other hand, are ordinary people with a need to access and navigate the internet. There could hardly be a greater disparity in relative bargaining strength.

Second, the Court may conclude that users have not unambiguously exhibited consent by accepting Google's terms of service. For example, in *Varela*, the Supreme Court considered whether the plaintiff was entitled to class arbitration. 139 S. Ct. at 1412. The Court declined to find the contract ambiguous and to apply *contra*

proferentem—thus requiring class arbitration—in the face of the foundational principle that "arbitration is a matter of consent." *Id.* at 1418. And an ambiguous contract could not manifest that consent. *See id.* That reasoning arguably applies to this case as well. Consumers should not be deemed to have consented to the collection and use of their personal information absent unambiguous contractual language. *See Brown*, 525 F. Supp. 3d at 1063 ("The disclosures must have only one plausible interpretation for a finding of consent."); *Calhoun I*, 526 F. Supp. 3d at 620 (same); *see also* H.B. 4, *supra* (providing that a consumer's consent must be unambiguous) (to be codified at Tex. Bus. & Com. Code § 541.001(6)). It is hard to see how such language is even arguably present here given that the district court required 7.5 hours of testimony from eight witnesses "[t]o better understand" the terms to which ordinary users supposedly agreed. *Calhoun II*, 645 F. Supp. 3d at 929.

Conclusion

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

Respectfully submitted.

Ken Paxton
Attorney General of Texas

Brent Webster
First Assistant Attorney General

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

Aaron L. Nielson
Solicitor General

/s/ Lanora C. Pettit
Lanora C. Pettit
Principal Deputy Solicitor General

Bill Davis
Deputy Solicitor General

Kyle D. Highful
Assistant Solicitor General

Counsel for Amici Curiae

Treg R. Taylor
Attorney General of Alaska

Kris Mayes
Attorney General of Arizona

Kathleen Jennings
Attorney General of Delaware

Anne E. Lopez
Attorney General of Hawai‘i

Theodore E. Rokita
Attorney General of Indiana

Brenna Bird
Attorney General of Iowa

Daniel Cameron
Attorney General of Kentucky

Jeff Landry
Attorney General of Louisiana

Anthony G. Brown
Attorney General of Maryland

Dana Nessel
Attorney General of Michigan

Lynn Fitch
Attorney General of Mississippi

Aaron D. Ford
Attorney General of Nevada

Raúl Torrez
Attorney General of New Mexico

Drew H. Wrigley
Attorney General of North Dakota

Dave Yost
Attorney General of Ohio

Marty J. Jackley
Attorney General of South Dakota

Sean D. Reyes
Attorney General of Utah

Jason S. Miyares
Attorney General of Virginia

Certificate of Service

On December 18, 2023, this brief was served via CM/ECF on all registered counsel and transmitted to the Clerk of the Court.

/s/ Lanora C. Pettit
Lanora C. Pettit

Certificate of Compliance

This brief complies with: (1) the type-volume limitation of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) because it contains 5,122 words, excluding the parts of the brief exempted by Rule 32(f); and (2) the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because it has been prepared in a proportionally spaced typeface (14-point Equity) using Microsoft Word (the same program used to calculate the word count).

/s/ Lanora C. Pettit
Lanora C. Pettit