No. 22-16993

IN THE

United States Court of Appeals
FOR THE NINTH CIRCUIT

PATRICK CALHOUN et al.,

Plaintiff-Appellants,

vs.

GOOGLE, LLC,

Defendant-Appellee,

On Appeal from the U.S. District Court
for the Northern District of California
No. 4:20-cv-05146-YGR (Hon. Yvonne Gonzales Rogers)

BRIEF OF AMERICAN ASSOCIATION FOR JUSTICE AND CONSUMER ATTORNEYS OF CALIFORNIA AS AMICI CURIAE IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

SAVEENA TAKHAR
Senior Legislative Counsel
CONSUMER ATTORNEYS OF CALIFORNIA
770 L Street, Suite 1200
Sacramento, CA 95814
(916) 442-6902
stakhar@caoc.org

SEAN DOMNICK
President
JEFFREY R. WHITE
Counsel of Record
AMERICAN ASSOCIATION FOR JUSTICE
777 6th Street, NW #200
Washington, DC 20001
(202) 617-5620
jeffrey.white@justice.org

Counsel for Amici Curiae

December 18, 2023

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, amicus curiae the American Association for Justice certify that it is a non-profit organization. It has no parent corporation or publicly owned corporation that owns 10% or more of its stock.

Respectfully submitted this 18th day of December 2023.

/s/ Jeffrey R. White

JEFFREY R. WHITE
Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

IDENTITY AND INTEREST OF AMICI CURIAE[1]

The American Association for Justice ("AAJ") is a voluntary bar association established in 1946 to strengthen the civil justice system, preserve the right to trial by jury, and protect access to the courts for those who have been wrongfully injured. With members in the United States, Canada, and abroad, AAJ is the world's largest plaintiff trial bar. AAJ members primarily represent plaintiffs in personal injury actions, employment rights cases, and other civil actions, including consumer privacy and data breach litigation. Throughout its 77-year history, AAJ has served as a leading advocate of the right of all Americans to seek legal recourse for wrongful injury.

Consumer Attorneys of California ("CAOC") is a voluntary membership organization representing over 3,000 associated consumer attorneys practicing throughout California. The organization was founded in 1962. Its membership consists primarily of attorneys who represent individuals who are harmed because of the negligent or wrongful acts of others. CAOC has taken a leading role in advancing and protecting the privacy rights of Californians in both the courts and the Legislature during the enactment of the California Consumer Privacy Act.

[1] All parties have consented to the filing of this brief. No party or party's counsel authored this brief in whole or in part. No person, other than amicus curiae, its members, and its counsel, contributed money that was intended to fund the preparation or submission of this brief.

AAJ, CAOC, and our members have a keen interest in the significant issues presented by this case regarding whether a consumer has knowingly consented to authorize access and use of their personal data.

SUMMARY OF ARGUMENT

1a. The crucial issue before the Court is whether online companies seeking a consumer's consent to the sharing and use of personal information must disclose their activities in terms that are unambiguously clear to reasonable users. Allowing companies to claim express authorization to harvest personal data based on a consumer clicking "I Agree" to multiple, misleading disclosures, as in this case, encourages "consent creep" that threatens to erode consumers' fundamental right to privacy.

Plaintiffs allege that Google promised the Chrome browser would not send their personal information to Google unless they chose to sync. Nevertheless, when they visited websites using the Chrome browser, Chrome transmitted that information to Google for its own purposes in violation of Google's express promises and California law. The District Court erred in granting summary judgment for Google and holding that Plaintiffs' express consent was effective and a complete defense.

Online privacy policies are standardized contracts of adhesion. They may be enforced based on adequate disclosure and the consumer's express consent.

California law requires that online companies seeking to harvest and use personal information obtain consent that is specific, informed, and unambiguous. If the online entity's disclosure is susceptible to more than one plausible interpretation, then the consumer's selection of "I Agree" is not specific, not fully informed, and is inherently ambiguous.

1b. Google clearly failed to obtain Plaintiffs' specific, informed, and unambiguous consent. Google's Chrome Privacy Notice ("CPN"), to which Plaintiffs agreed, assured Chrome users that their personal information would not be sent to Google unless they chose to sync Chrome with their Google Account. However, Plaintiffs allege that although they did not sync to their Google Account, their personal information was sent to Google anyway. Although the District Court relied on a few statements from the Google Privacy Policy, there is clearly more than one plausible interpretation of the scope of Plaintiffs' consent.

At best for Google, the documents are ambiguous, a conclusion that finds support in the fact that two district court judges in this case came to diametrically opposite interpretations. Denying Google's motion to dismiss, Judge Koh found that a reasonable user could interpret the disclosures as allowing users to limit the scope of their consent by declining to sync. Judge Rogers, relying in part on extrinsic evidence, held that the Chrome Privacy Notice was not applicable, and Google's activities fell within Google's disclosures under the General Privacy Policy. The text

of the Consent Bump Agreement and the New Account Creation Agreement likewise supports the plausibility of Plaintiffs' alternative interpretation of the scope of their consent.

2a. Abusive privacy policies present a growing danger to consumers' privacy rights when they go online. The right of privacy is a fundamental right guaranteed by the California Constitution and the state legislature has enacted statutory protections of individuals' personal information online.

2b. Consumers' personal information is highly valuable, and online companies seeking to harvest personal data, including Google, have made aggressive use of adhesive privacy policy "agreements" to obtain consent. Privacy policies are contracts of adhesion on steroids, with no limit on their length or complexity. Consumers completing an online transaction cannot negotiate; they seldom even read the terms to which they click "I Agree." Yet the District Court in this case allowed such a privacy policy to operate as effective consent to the use of personal information.

In this case, the District Court erroneously determined that the Chrome Privacy Notice, with its assurance that users could preclude the harvesting of their personal information, was inapplicable, essentially adopting Google's interpretation of its own document. In fact, the more reasonable reading of the plain text is that the CPN is the only document that matters. That is because the Google Terms of Use (to

which Plaintiffs also "agreed") expressly state that, if there is a conflict, the Chrome Privacy Notice governs the rules for the Chrome browser.

This Court can protect the privacy rights of consumers by insisting upon strict application of the common-law rule of contract construction, *contra proferentem*. That widely accepted rule, that any uncertainty or ambiguity in a written contract must be resolved against the drafter, serves an important public policy of protecting consumers by incentivizing companies to draft privacy agreements that are clear and unambiguous. To adopt the company's interpretation of the notifications it presents to users to obtain their "I Agree" is to invite companies to insert ever-increasing intrusions into privacy "agreements." With each advance of such "consent creep," the reasonable expectations of privacy for online consumers further diminish.

3. One step to advance consumer protection is to instruct district courts to submit disputed questions regarding the scope of online express consent to the jury. The scope of effective consent is clearly a question of fact, determined by reasonable expectations of privacy. Where, as here, the scope of consent requires a factual construction of the defendant's online disclosures, the standard is that of the reasonable user. The jury is the appropriate decisionmaker due to its unique competence in ascertaining reasonableness, and summary judgment in such cases is not appropriate. In this case, the interpretation of privacy agreements requires

extrinsic evidence and expert testimony and the jury in its role as assessor of credibility, is the appropriate decisionmaker.

The right to trial by jury is enshrined in the Seventh Amendment because of the Founders' faith in the common sense and experience of ordinary citizens. They anticipated and welcomed the fact that citizen jurors would at times view evidence and decide cases differently than judges. Jurors keep the administration of the law in accord with the views of the community. Today, Americans who serve as jurors are as likely as judges to understand even complex scientific issues.

This Court has indicated that, where a factual question is presented, a district court may properly submit the question of the contract's meaning to the jury. This Court should hold that a jury determination of the scope of a user's consent to the sharing of private information based on how a reasonable user would interpret ambiguous or inconsistent privacy policy agreements is both appropriate and required. In this way, ordinary citizens can keep "consent" grounded in the practicalities and notions of fairness of the community.

ARGUMENT

I. ONLINE COMPANIES SEEKING TO HARVEST AND USE CONSUMERS' PERSONAL INFORMATION MUST OBTAIN SPECIFIC, INFORMED, AND UNAMBIGUOUS CONSENT.

Amici address this Court with respect to the crucial issue in this case: Whether online commercial actors who intend to harvest and use a consumer's personal

information are required to make sufficiently clear disclosures to ensure that the consumer's consent is specific, informed, and unambiguous. Failure to ensure that online user "agreements" are understandable to the ordinary person invites companies to load increasingly intrusive terms under the guise of "privacy agreements." Such "consent creep" threatens to erode consumers' reasonable expectations of online privacy.

A. Effective Consent to Online Use of Personal Information Must Be Specific, Informed, and Unambiguous.

Plaintiffs contend that when they used Chrome to communicate with websites, Chrome did not simply use their information locally for purposes of facilitating that communication. Instead, a copy of that personal information, which Plaintiffs allege included financial, medical, and political communications, was also sent to Google for its own commercial and advertising use in violation of California law. First Amended Complaint ["FAC"] ¶ 152. However, in using the Chrome browser, Plaintiffs and Google were subject to the Chrome Privacy Notice, which expressly promised, "the personal information that Chrome stores [including "browsing history information" and "cookies or data from websites that you visit"] won't be sent to Google unless you choose to store that data in your Google Account by turning on sync."

Ignoring the language of the Chrome Privacy Notice, the lower court below granted summary judgment for Defendant, holding that Plaintiffs' express consent

to this use of their personal information by Google was a complete defense. Specifically, the District Court held that by clicking on "I Agree" to the terms set out in Google's Terms of Service, General Privacy Policy, and other documents, Plaintiffs gave effective consent that barred their privacy claims. *Calhoun v. Google, LLC*, No. 20-CV-5146-YGR, 2022 WL 18107184, at *16-17 (N.D. Cal. Dec. 12, 2022) (Slip Op.).

Importantly, "privacy policies are typically recognized as contracts." Oren Bar-Gill et al., *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. Chi. L. Rev. 7, 28 (2017) (emphasis omitted). They are standardized and non-negotiated contracts of adhesion, enforceable based solely on the consumer's express agreement, provided that the consumer was clearly and specifically notified of the practice to which they were agreeing. *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014); *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *14 (N.D. Cal. Sept. 26, 2013).

The California Consumer Privacy Act, enacted in 2018 in response to the Cambridge Analytica scandal, has been heralded as "one of the most significant regulations overseeing the data-collection practices of technology companies in the United States." Luis Miguel M. del Rosario, *On the Propertization of Data and the Harmonization Imperative*, 90 Fordham L. Rev. 1699, 1720 (2022) (quoting Daisuke

Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. Times (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html).

In 2020, California voters strengthened the requirements for actual consent by approving Proposition 24 to enact the California Privacy Rights Act (CPRA). As amended, California law defines consent as

> [F]reely given, *specific, informed, and unambiguous* indication of the consumer's wishes by which the consumer, . . . signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent.

Cal. Civ. Code § 1798.140 (emphasis added). This statutory language "ensures that consent is freely given and is not obtained through confusing or misleading methods" and that the use of personal information is "clearly and conspicuously disclosed to the user." Sen. Comm. on Judiciary, Analysis of A.B. 1262, 2021-2022 Reg. Sess., at 5, 11 (Cal. Jan. 10, 2022).

Thus, online companies can rely on users' assent to privacy policies only so long as their disclosures regarding personal data have only one "plausible interpretation." *In re: Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019). The District Court below, initially denying

Google's motion to dismiss, properly applied this standard. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620–21 (N.D. Cal. 2021).

On motion for summary judgment, however, a different judge disregarded that test. The Court noted that Plaintiffs clicked "I Agree" to Google's General Privacy Policy and related documents and that "a reasonable user reviewing these same disclosures would understand that Google" notified users that it engages in the complained-of conduct. Slip Op. at *13. The District Court did not determine that this is the only plausible interpretation of the pertinent documents. In fact, the Court acknowledged Plaintiffs' alternative reading, but merely contended that Plaintiffs' interpretation was based on "cherry-picked" statements. *Id.* at *15.

B. Google Failed to Obtain Specific, Informed, and Unambiguous Consent to Transmit Plaintiffs' Personal Information to Google.

The District Court determined that the relevant documents affecting users' consent to the harvesting and use of personal information are Google's Terms of Service, General Privacy Policy, Chrome Privacy Notice, Consent Bump Agreement, and New Account Creation Agreement. Slip Op. at *2. And the parties do not dispute that Plaintiffs agreed to those documents. *Id*. at *8.

Whether the terms of a contract are ambiguous is a question of law, reviewable by this Court *de novo*. *Kunin v. Benefit Tr. Life Ins. Co.,* 910 F.2d 534, 537 (9th Cir. 1990). In this case it is clear that these disclosures, as they relate to whether Chrome will send personal information are, at best for Google, contradictory on their face.

The CPN, which is specifically applicable to users of the Chrome browser, states: "When you sign in to the Chrome browser or a Chromebook *and enable sync with your Google Account*, your personal information is saved in your Google Account on Google's servers . . . [and] will be used and protected in accordance with the Google Privacy Policy." Slip Op. at *5 (emphasis added). The CPN expressly assures users that "the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you." Slip Op. at *4. "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.* (emphasis added).

Google's General Privacy Policy ("GPP") states that, in certain scenarios, Google may collect, store, and use that user's personal information. Slip Op. at *3-4. However, the same document says nothing about what Chrome will send to Google (a different act than collection) and expressly limits what Google will collect from the Chrome browser.

Reading both documents in their entirety, Google consistently promised users that Chrome would not send their personal information to Google unless they chose to sync—and Google would not collect or save Chrome browsing history to a person's Google Account unless they "enabled Chrome sync."

At best for Google, the two notices are in direct conflict. However, because

Plaintiffs clicked on "I Agree" to both, what they agreed to is inherently non-specific, not fully informed, and inherently ambiguous.

District Judge Koh, denying Google's motion to dismiss this action, found that, "a reasonable user could have concluded that using Chrome without sync was a way to control 'the information that's collected, stored, and shared when you use the Google Chrome browser.'" 526 F. Supp. 3d at 621 (quoting the CPN). Furthermore, "a reasonable user could have concluded that if he or she used Chrome without sync, his or her personal information would *not* be sent to Google." *Id.* (emphasis added).

On motion for summary judgment, District Judge Rogers also acknowledged the inconsistency in Google's privacy agreements, noting that the determination of "which agreement controls the at-issue data collection" is a core issue in this case. Slip Op. at *8. Although Judge Rogers found that two additional documents support Google's broad interpretation of consent, they clearly support Plaintiffs' interpretation as well.

In particular, the Consent Bump Agreement explains that Google has introduced "some new features *for your Google Account,*" that this change will "let Google use data *in your account* to improve the relevance of ads that appear in Google products," and that the user "can find and control that data *in My Account*," where the user can choose to sync. *See* Slip Op. at *5, *6 (emphasis added). The

New Account Creation Agreement provides: "*Depending on your account settings*, some of this data *may* be associated with your Google Account and we treat this data as personal information. . . . You can control how we collect and use this data *at My Account* (myaccount.google.com)." *Id.* at *6 (emphasis added).

A plausible reading by a reasonable user is that both documents relate only to the personal information of users who have chosen to sync with their Google Account. Google clearly failed to carry its burden of showing that Plaintiffs' consent was specific, informed, and unambiguous.

The District Court gave no regard to this Court's guidance in *In re: Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020). The Court there examined Facebook's assurance to users who visit a website with a Facebook social plug in: "If you are logged into Facebook, we also see your user ID number and email address. . . . If you log out of Facebook, we will not receive this information about partner websites." *Id.* at 602. This Court concluded that, regardless of any expression of general consent, "a user might assume that only logged-in user data would be collected. . . . Plaintiffs have plausibly alleged that Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway." *Id.*

Instead, the District Court here rejected Plaintiffs' plausible reading in favor of Google's interpretation of its own handiwork. The Court's grant of summary judgment invites online companies to lard their privacy policies with vague,

inconsistent, and even contradictory representations with confidence that courts will allow them to stretch "I Agree" into effective consent. Strict construction of such documents against the drafters is needed to deter such abuses.

II. ABUSIVE PRIVACY POLICY "AGREEMENTS" PRESENT A GROWING DANGER TO THE PRIVACY RIGHTS OF CONSUMERS ONLINE.

A. The Right to Privacy of Personal Information Is Fundamental Under California Law.

Among the fundamental and inalienable rights the People of California have secured for themselves is the right to personal privacy. In 1972, California voters amended the state's Constitution to affirmatively safeguard each person's "reasonable expectation of privacy." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 36–37 (1994) (citing Cal. Const. art. I, § 1). Additionally, as this Court has observed, the California legislature has acted to "codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing" to sue. *In re: Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 598; *see also Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117 (9th Cir. 2020).

Essential to privacy is the right to keep personal information personal. The California legislature expressly found in the Information Practices Act of 1977, that with the advance of information technology, the individual's "right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information," by state agencies, making it "necessary that the

maintenance and dissemination of personal information be subject to strict limits." Cal. Civ. Code § 1798.1.

This Court as well has recognized the privacy right "encompass[es] the individual's control of information concerning his or her person." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (quoting *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989)). As has happened repeatedly in our history, "advances in technology can increase the potential for unreasonable intrusions into personal privacy." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019).

B. California Consumers' Fundamental Right of Privacy Is Endangered by Online Entities Seeking to Harvest Valuable Personal Information.

Personal information is a tremendously valuable commodity. Two decades ago, one scholar warned: "The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056 (2004). Indeed, prospecting for personal data has become the 21st Century's gold rush. *See The World's Most Valuable Resource Is No Longer Oil, But Data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

With huge profits to be had and the application of traditional legal protections to internet transactions unsettled, tech companies have sometimes abused their access to online personal data. One extreme example was Cambridge Analytica's harvesting of user data on the Facebook platform, and the subsequent microtargeting of political ads that followed during the 2016 presidential election. In response, the Federal Trade Commission (FTC) levied a record-setting $5 billion penalty against Facebook, the largest privacy or data security penalty ever imposed. *See* Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. Rev. 1252, 1254–55 (2022). The scandal prompted enactment of the California Consumer Privacy Act. *See* Cathy Lee, *The Aftermath of Cambridge Analytica: A Primer on Online Consumer Data Privacy*, 48 AIPLA Q.J. 529, 536 (2020).

The defendant in this case is a leader in this online gold rush. Today, Google is not so much a search engine, as it is the world's largest digital advertising agency. In 2022, Google brought in revenues of $280 billion, making it the fourth largest corporation on the planet. Over 80% of that income, $224.47 billion, came from advertising. *See Advertising Revenue of Google from 2001 to 2022*, Statista (Feb. 2023), https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

That growing river of revenue is made possible by Google's harvesting of users' personal data. Google tailors its advertisements to target the users most likely

to buy what a specific advertiser is selling, greatly enhancing what those advertisers will pay. *See* Megan Graham & Jennifer Elias, *How Google's $150 Billion Advertising Business Works*, CNBC (Oct. 13, 2021), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html.

Online companies found that the most effective immunity from even the most stringent privacy protections enacted by state and federal governments is user "consent." Frequently framed as "privacy policies," these are contracts in which the user "agrees" to the harvesting and use of their personal information in return for the use of the online service, such as Google's search engine. They are contracts of adhesion on steroids—wholly unconstrained by physical limits of time and space. There is literally no limit on the length and complexity or the layers of menus and hyperlinks that drafters can build into these obstacles placed in the paths of online consumers.

For a court to allow the drafter of such a one-sided contract—which cannot be changed and the consumer will likely not read—to insist that "I Agree" equals valid consent "is akin to allowing a robber to call a mugging a donation." Nancy S. Kim, *Adhesive Terms and Reasonable Notice*, 53 Seton Hall L. Rev. 85, 88 (2022); *see also* Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23(1) Info., Comm. & Soc'y 128, 128–47 (2020), https://papers.ssrn.com/

sol3/papers.cfm?abstract_id=2757465. But that is not a far reach from the District Court's summary judgment decision below.

C. The District Court Erred in Holding That the Chrome Privacy Notice, Including Its Assurance That Users Could Prevent Sending Their Personal Information to Google, Is Inapplicable.

A core issue in this case is whether Plaintiffs' consent was governed by: (1) the specific Chrome Privacy Notice, which applies in the event of any conflict per Google's Terms and plainly states that personal data would be sent to Google only if the user synced to their Google Account; or (2) Google's general Privacy Policy, which notifies users that Google may collect and use personal information in certain scenarios. *See* Slip Op. at *8.

Google argued that Chrome's assurance to users applied only to "features specific to Chrome." *Id.* at *8–9. The District Court agreed and, following a day-long evidentiary hearing, determined that Google's collection and use of personal information was "not specific to Chrome, but browser-agnostic." *Id.* at *10. That is, other browsers also caused personal information to be shared with Google. The District Court concluded, therefore, that the CPN and its assurance that users could protect personal information was not applicable. *Id.* at 15.

However, the plain text of the CPN Google's own document supports Plaintiffs' opposing interpretation. The full sentence relied on by the District Court states: "Although this policy describes features that are specific to Chrome, any

personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the Google Privacy Policy, as changed from time to time." Chrome Privacy Notice, Google (May 20, 2020).

Nowhere does the text support Google's and the District Court's interpretation that the CPN applies *only* to features that are specific to Chrome. Moreover, the only "features specific to Chrome" identified in the CPN are the Safe Browsing features. Those features allow a user to send *additional* information to Google for review to guard against phishing, malware, or other potential dangers of visited websites. *Id.* The above-quoted provision indicates that such additional information provided by the user to Google or stored in the user's Google Account will be subject to the General Privacy Policy. Nowhere is there any negation of the representation to users that they can prevent the transmission of their personal information to Google by simply declining to sync to their Google Account.

This reading is not only plausible, but it is indeed more reasonable than the tortured construction adopted by the District Court. First, it is based on the plain text of Google's CPN, not on the behavior of other browsers. Second, it gives effect to Google's Terms of Service, which provide that where "these terms conflict with the service-specific additional terms, the additional terms will govern for that service." *See* Slip Op. at *2.

Finally, adoption of Plaintiffs' interpretation of Google's privacy agreements

comports with the common-law canon of contract construction, *contra proferentem*, which "is followed in all fifty states and the District of Columbia, and with good reason." *Kunin*, 910 F.2d at 540. *See, e.g.*, *City of Hope Nat'l Med. Ctr. v. Genentech, Inc.*, 181 P.3d 142, 158 (Cal. 2008). This Court has paraphrased this rule as "when one party is responsible for the drafting of an instrument . . . any ambiguity will be resolved against the drafter." *Kunin*, 910 F.2d at 538–39. An important policy served by the rule when construing standardized contracts of adhesion is "to protect the public against institutions that are inclined to draft obscure contracts to entrap consumers." Ethan J. Leib & Steve Thel, *Contra Proferentem and the Role of the Jury in Contract Interpretation,* 87 Temp L. Rev. 773, 776 (2015).

By rejecting Plaintiffs' reasonable interpretation and adopting Google's reading of its own consent documents, the District Court has established a strong incentive for online entities to load more self-serving content into their privacy policies, which are not negotiated, or even read, by users. *See generally* Obar & Oeldorf-Hirsch, *supra*. Under these circumstances, online companies can be confident of obtaining "consent" for intrusions far beyond what reasonable users might agree to. As a result, one observer has warned, "an absurd situation is created: instead of being a tool that protects users from the risks of using digital apps, [privacy policies] have become tools that legalize all app providers' actions, even those that are considered unethical, because the users have allegedly consented to

them." Bar Fargon Mizrahi, *Risky Fine Print: A Novel Typology of Ethical Risks in Mobile App User Agreements*, 66 Vill. L. Rev. 483, 492 (2021). With each advance of such "consent creep," the reasonable expectations of privacy for online consumers shrink further.

Courts can play a role in protecting consumers' fundamental privacy rights. As this Court has suggested: "As millions of Americans increasingly conduct their affairs online, 'the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data . . . is untenable.'" *In re: Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 598 (quoting *In re: Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3rd Cir. 2019)).

One important step this Court can take to protect consumers from unreasonably one-sided and misleading privacy policies purporting to obtain "consent" to the harvesting of personal information is to submit disputes over the interpretation of such agreements to the jury.

III. THE SCOPE OF CONSENT IS A QUESTION OF FACT THAT SHOULD BE DECIDED BY A JURY.

A. The Scope of Express Consent Is a Question of Fact Measured by the Objective Standard of the Reasonable Person, Which Is Most Appropriately Decided by the Jury.

The conclusive issue before this Court is whether Google's conduct falls within the scope of Plaintiffs' express consent and, importantly, whether that determination should be made by the District Court or by the jury.

Even where users have given their express consent to intrusions into their privacy, ascertaining the scope of that consent is a factual determination. *See, e.g.*, *Fraley v. Facebook, Inc*., 830 F. Supp. 2d 785, 806 (N.D. Cal. 2011) ("[W]hether Facebook's Statement of Rights and Responsibilities, Privacy Policy, or Help Center pages unambiguously give Defendant the right to use Plaintiffs' names, images, and likenesses . . . for Facebook's commercial gain remains a disputed question of fact . . . ."); *In re: Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *15 (N.D. Cal. Mar. 18, 2014) ("[E]xpress consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the interceptions.") (citations omitted).

The scope of a consumer's consent may be defined by the zone of their reasonable expectations of privacy. *See Javier v. Assurance IQ, LLC*, No. 4:20-CV-02860-JSW, 2021 WL 940319, at *2 (N.D. Cal. Mar. 9, 2021) ("Consent generally defeats privacy claims . . . because a party that consents to having information collected has no reasonable expectation of privacy.") (citing *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016)). Where consent requires application of this objective "reasonable person" standard, the jury is the appropriate decisionmaker. Thus, whether an intrusion violated the plaintiff's "objectively reasonable" expectations of privacy, and thus exceeded the scope of consent, "is a

question for the jury, not this Court." *Opperman*, 205 F. Supp. 3d at 1077. *See also Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 233–34 (Cal. 1998) (holding that whether an auto accident victim had a reasonable expectation of privacy that was violated by a news gatherer's recording of emergency medical response was a "question[ ] for the jury"); *Steele v. RadioShack Corp.*, No. 11-14021, 2012 WL 368329, at *5 (E.D. Mich. Feb. 3, 2012) (holding that, where a plaintiff left his phone with the defendant to transfer data to a new phone, whether dissemination of that data to plaintiff's employer was "within the scope of consent is a question of fact for a jury to decide").

In addition, as the District Court here recognized, where the scope of plaintiffs' consent is defined by the privacy disclosures to which plaintiffs agreed, the proper standard by which those documents must be interpreted is that of the "reasonable user." *E.g.*, Slip Op. at *13; 526 F. Supp. 3d at 621. It is the role of ordinary citizens serving as jurors to apply that standard as well.

For that reason, this Court has repeatedly instructed that "summary judgment is generally an inappropriate way to decide questions of reasonableness because 'the jury's unique competence in applying the 'reasonable man' standard is thought ordinarily to preclude summary judgment.'" *Gorman v. Wolpoff & Abramson, LLP*, 584 F.3d 1147, 1157 (9th Cir. 2009) (quoting *In re Software Toolworks, Inc.*, 50 F.3d 615, 621 (9th Cir. 1994)). *See also Eid v. Alaska Airlines, Inc.*, 621 F.3d 858,

868 (9th Cir. 2010). The circumstances in which summary judgment might be appropriate on a determination of reasonableness are extremely limited to those instances where "no rational jury" could come to any other conclusion. 50 F.3d at 622. This is not such a case.

B. Where Determining the Scope of Consent Depends upon Assessment of Extrinsic Evidence, Such Determination Is Most Appropriate for the Jury.

On Google's privacy documents alone, the District Court conducted a day-long hearing on the matter, receiving live testimony from eight witnesses and relying on declarations of several others. *See* Slip Op. at *9. The District Court concluded based on this parol evidence that the scope of Plaintiffs' consent was defined by the General Privacy Policy, not the Chrome Privacy Notice. That determination, too, was properly for the jury.

As the California Court of Appeal recently restated, when the terms of a contract are uncertain, it is the duty of the trial court to give the parties "a full opportunity to produce evidence of the facts, circumstances and conditions," after which proper interpretation "presents a question of fact which is inappropriate for summary judgment." *Visitacion Inv., LLC v. 424 Jessie Historic Properties, LLC*, 92 Cal. App. 5th 1081, 1093 (Cal. Ct. App. 2023) (quoting *Rogers v. Prudential Insurance Co.*, 218 Cal. App. 3d 1132, 1136–37 (Cal. Ct. App. 1990)). *See also City of Hope Nat'l Med. Ctr.*, 181 P.3d at 157 ("This rule—that the *jury* may interpret an

agreement when construction turns on the credibility of extrinsic evidence—is well established in our case law.") (emphasis added).

C. Disputes Regarding the Scope of Online Consent Should Be Submitted to the Jury.

This Court should enhance consumers' protection against unwanted intrusions on their privacy rights under the guise of adhesive "consent" by restoring the role of the jury in interpreting such agreements. This is "a fact-based inquiry that is within the everyday experience of consumers" sitting as jurors. Kim, *supra*, at 101. Unfortunately, "the result of judges making factual determinations better left to juries is that some courts have concluded that [users] should respond to adhesive digital terms in a way that no reasonable consumer does or should be expected to behave." *Id.*

The right to a jury determination of the fact in a civil case is guaranteed by the Seventh Amendment. Under federal law, that right must "be preserved to the parties inviolate." Fed. R. Civ. Pro. 38(a); *see also* Cal. Const. art. I, § 16 ("Trial by jury is an inviolate right and shall be secured to all.").

As Justice Ginsberg noted, an "essential characteristic" of our civil justice system is that, "under the influence—if not the command—of the Seventh Amendment, [it] assigns the decisions of disputed questions of fact to the jury." *Gasperini v. Ctr. for Humans., Inc.*, 518 U.S. 415, 432 (1996) (quoting *Byrd v. Blue Ridge Rural Elec. Co-op., Inc.*, 356 U.S. 525, 537 (1958)).

The reason the jury's role is enshrined in the Constitution itself, Chief Justice Rehnquist explained, is that "[t]he founders of our Nation considered the right of trial by jury in civil cases" to be "a safeguard too precious to be left to the whim . . . of the judiciary." *Parklane Hosiery Co. v. Shore*, 439 U.S. 322, 339 (1979) (Rehnquist, J., dissenting). They "believed that a jury would reach a result that a judge either could not or would not reach." *Id.* at 344. "Trial by a jury of laymen rather than by the sovereign's judges was important to the founders because juries represent the layman's common sense, . . . and thus keep the administration of law in accord with the wishes and feelings of the community." *Id.* at 343–44 (quoting Oliver Wendell Holmes, *Law in Science and Science in Law*, *in* Collected Legal Papers 237 (1920)).

The Supreme Court has repeatedly emphasized that the jury is the essential finder of fact: "Maintenance of the jury as a fact-finding body is of such importance and occupies so firm a place in our history and jurisprudence that any seeming curtailment of the right to a jury trial should be scrutinized with the utmost care." *Dimmick v. Schiedt*, 293 U.S. 474, 486 (1935). *See also Beacon Theatres, Inc. v. Westover*, 359 U.S. 500, 501 (1959); *Chauffeurs, Teamsters and Helpers, Loc. No. 391 v. Terry*, 494 U.S. 558, 565 (1990).

Judicial reluctance to allow juries to make findings regarding the interpretation of contracts is outmoded and largely a holdover from a time when

"jurors were often illiterate." Restatement (Second) of Contracts § 212 cmt. d (Am. L. Inst. 1981).

Today, a cross-section of Americans selected to serve as jurors is not so ill-equipped, even with respect to difficult scientific matters, as one trial judge has suggested. *See* Ronald W. Tochterman, Daubert*: A (California) Trial Judge Dissents*, 30 U.C. Davis L. Rev. 1013, 1019 (1997). Empirical evidence, including research conducted by the Federal Judicial Center, "consistently points to the general competence of the jury," and shows that "juries are capable of deciding even very complex cases." Joe S. Cecil, Valerie P. Hans, & Elizabeth C. Wiggins, *Citizen Comprehension of Difficult Issues: Lessons from Civil Jury Trials*, 40 Am. U. L. Rev. 728, 745, 764 (1991).

This Court has indicated that, where a factual question is presented, a district court may "properly submit[] the question of the contract's meaning to the jury." *Rich v. Outdoor Media Dimensions, Inc.*, 183 F. App'x 655, 656 (9th Cir. 2006). Where the scope of an online consumer's express consent is in dispute, as in this case, this Court should instruct that a jury determination is both appropriate and required.

For example, the District Court properly respected the role of the jury in a similar case, *Opperman v. Path*. *See* 205 F. Supp. 3d 1064. Plaintiffs there alleged that app developer Yelp had illegally uploaded data from their "Contacts" address

book. Yelp asserted that users agreed to Yelp's privacy policy which disclosed that Yelp would "[f]ind friends on Yelp using your Contacts." The District Court found that a reasonable user could construe this as consent to use of their Contacts information locally on the user's phone to match them with friends. But whether the scope of Plaintiffs' express consent included "effective consent to upload the users' Contacts data as opposed to just accessing it locally . . . is an issue for the jury." *Id.* at 1073. Summary judgment was therefore inappropriate. *Id.* at 1074–75.

Submission of such disputes to the jury presents an effective deterrence to the extraction of "consent" from consumers by unfair privacy policies.

CONCLUSION

For the foregoing reasons, AAJ and CAOC urge this Court to reverse the judgment of the District Court below.

Respectfully submitted,

/s/ Jeffrey R. White
JEFFREY R. WHITE
AMERICAN ASSOCIATION FOR JUSTICE
777 6th Street, NW #200
Washington, DC 20001
(202) 617-5620
Jeffrey.White@justice.org

Counsel for Amici Curiae
American Association for Justice and
Consumer Attorneys of California

Dated: December 18, 2023

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 29(a)(5) and Circuit Rule 29-2 because this brief contains 6,500 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f). I further certify that this brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word for Microsoft 365 in 14-point Times New Roman type style.

Date: December 18, 2023

/s/ Jeffrey R. White
JEFFREY R. WHITE

CERTIFICATE OF SERVICE

I, Jeffrey R. White, counsel for amici curiae and a member of the Bar of this Court, hereby certify that on December 18, 2023, electronically filed the foregoing document with the Clerk of Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. I also certify that the foregoing document is being served on this day on all counsel of record via transmission of the Notice of Electronic Filing generated by CM/ECF. All participants in this case are registered CM/ECF users.

/s/ Jeffrey R. White
JEFFREY R. WHITE

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 18. Certificate for Paper Copy of Electronic Brief

Instructions for this form: http://www.ca9.uscourts.gov/forms/form18instructions.pdf

9th Cir. Case Number(s) 22-16993

My name is Jeffrey R. White

I certify that this brief is identical to the version submitted electronically on *(date)*:

December 18, 2023.

Signature s/ Jeffrey R. White **Date** Dec 18, 2023

(either manual signature or "s/[typed name]*" is acceptable)*