No. 22-16993

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

PATRICK CALHOUN, ET AL.,
Plaintiffs-Appellants,

v.

GOOGLE, LLC,
Defendant-Appellee.

On Appeal from the United States District Court for the
Northern District of California
No. 20-cv-5146-YGR
The Honorable Yvonne Gonzalez Rogers,
District Court Judge

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Alan Butler
Sara Geoghegan
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

Attorneys for Amicus Curiae

December 21, 2023

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC regularly participates as *amicus* in this Court and other courts in cases concerning privacy rights and harmful data practices. EPIC also regularly advocates for meaningful regulation of extractive, invasive, and unfair data collection and profiling systems. EPIC is interested in this case because of EPIC's concern that the internet's digital commercial surveillance systems rely on harmful data practices and invade users' privacy. EPIC previously filed an *amicus* brief on generic notices being insufficient to establish meaningful consent for data practices in *Smith v. Facebook, Inc*., 745 F. App'x 8 (9th Cir. 2018).[1]

[1] Both parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no party or party's counsel authored this brief in whole or in part nor contributed money intended to fund the preparation of this brief. No outside person contributed money intended to fund the preparation of this brief.

SUMMARY OF THE ARGUMENT

For more than two decades, Google and other internet companies have presented privacy as an issue of "user choice" and argued that their legal obligations should only extend so far as the promises they have explicitly made in their policies, terms of service, and other statements. This "notice and choice" framework has led to a massive expansion in commercial surveillance that has fueled harmful discrimination, enabled invasive profiling, and degraded user privacy across the internet ecosystem. In response to the recent trend of users demanding greater privacy protection, companies like Google have made new privacy promises and offered new services that they claim protect user privacy. This case is about what happens when a company purports to offer its users new privacy-protective settings on the one hand, but then continues to invade their privacy on the other.

Under the traditional consent regime that courts have applied in common law privacy cases, companies get to set the terms of data collection, and users are left to navigate a byzantine structure of interlinked legal documents and complex settings to attempt to preserve some degree of control over their data. But in this case, Google

has gone so far as to reject even that minimal layer of protection. Google contends that even when it has explicitly promised its users that it will protect their data, it doesn't have to abide by that promise so long as it points to contrary terms in its general user agreement and statements posted in a sprawling web of disclosure pages.

The ruling in favor of Google below is a fundamental rejection of the reasonable consumer standard and would eliminate even the modicum of privacy that the common law currently provides to internet users. This brief sets out three reasons why the district court erred in its decision to grant Google's motion for summary judgment and explains why the mere existence of a broad, permissive clause in Google's general terms of service cannot and does not constitute actual consent in this case.

First, when Google makes specific privacy promises to Chrome users, the company should not be allowed to override those promises with blanket disclaimers in its general user agreement. To permit this would be inconsistent with traditional contract interpretation principles and ignore the reasonable consumer expectation standard applied in common law and consumer protection cases. Second, internet users

want strong privacy protections online and companies like Google should not be insulated from liability when they expand the scope of their disclosures beyond what users reasonably expect. Granting an affirmative consent defense in this case invites a race to the bottom: companies will, and have, followed suit to use unfair and deceptive practices to continue to extract personal information from users online. Third, the defense of affirmative consent should (indeed, does) require more than mere disclosure. The notice and choice regime promoted by Google and other online providers over the last three decades has prevented users from exercising meaningful agency or consent over how their data is handled. Yet the district court's decision doubles down on the failed notice and choice regime, allowing a company to quietly rescind its specific promise to users through a contrary term in a general privacy policy—and more, to infer a user's consent to that change. The Court should decline Google's invitation to drain the word "consent" of all meaning and reverse the order of the district court.

ARGUMENT

This case presents the question of whether the existence of general disclosures in Google's terms of service that conflict with

specific promises of heightened privacy protections provided to Chrome users is sufficient, as a matter of law, to establish the affirmative defense of consent. Specifically, the question is whether Google can assert the consent defense as to its collection of personal information about Chrome users' online activities and browsing histories, despite the specific promises made to those users in its Chrome Privacy Notice not to collect such data. Whether a reasonable user would have understood that Google was tracking the browsing behavior of Chrome users is a fact-intensive inquiry that the district court should have considered in light of all of the privacy statements made by the company. The district court should not have granted summary judgment based on the record for the reasons set out below.

In recent years, Google and other online tech companies have repeatedly undermined user privacy online by collecting huge volumes of personal information and using it to track and profile users. This constant tracking has fueled harmful data practices, including discrimination and invasions of the most intimate details of users' lives. Yet companies have at every turn attempted to disclaim liability for

their commercial surveillance practices based on vague and general statements in their terms of service.

I. COURTS SHOULD GIVE SUBSTANTIAL WEIGHT TO A COMPANY'S STATEMENTS PROMISING HEIGHTENED PRIVACY PROTECTION WHEN EVALUATING AN ASSERTED CONSENT DEFENSE

The key issue in this case is whether Google can successfully assert the affirmative defense of consent where the company made specific promises to protect the privacy of Chrome users' browsing history that conflicted with the company's general privacy disclosure. The answer to this question, plainly, is no—for three reasons.

First, the record does not establish that a "reasonable user" would have understood Google's general privacy disclosure to rescind the company's express commitments to Chrome users, let alone that Chrome users consented to that rescission. Second, the district court focused erroneously on the data practices of *other* browsers to conclude that the privacy promises made to Chrome users were effectively meaningless—and that Chrome users had actually consented to less favorable privacy terms. This warped understanding of "consent" ignores the vast information and power asymmetry in Google's relationship with its users, which allows the company to obfuscate its

data practices one minute and assume full user knowledge of those practices the next. Finally, to the extent that this case forces the Court to address a novel question of law—can a party successfully mount an affirmative defense of implied consent if a general disclosure is in apparent conflict with a specific promise to the user?—the Court must make clear to Google and companies engaging in similar practices that disclaiming specific promises to a user through general disclosures eliminates implied consent as a defense.

The record simply does not support the conclusion that Chrome users consented to the collection of their personal data. In common law and statutory privacy cases, this Court has recognized a limited affirmative defense of consent when the court finds that the circumstances, considered as a whole, show that a "reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization." *Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018). But the burden is on the party seeking the consent defense to prove consent exists, *Matera v. Google Inc.*, No. 15-cv-4062, 2016 WL 5339806, at *17 (N.D. Cal. Sept. 23, 2016), and the Ninth Circuit requires that any consent be actual,

whether express or implied. *In re Google, Inc.*, No. 13-md-2430, 2013 WL 5423918, at *12 (N.D. Cal Sept. 26, 2013). Although courts have sometimes held that disclosures in a terms a service or clickwrap-style contract can be used to establish consent, the disclosures must "explicitly notify" users of the conduct at issue. *Id.* at *13. Indeed, the disclosures must provide users notice of the "specific practice" at issue. *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014). In the tort context, the consent defense is only available when the defendant can show that the plaintiff consented "to the particular conduct, or to substantially the same conduct" and if the alleged tortfeasor does not exceed the scope of that consent. Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4.

Here, Google's assertion of an implied consent defense fails. The burden is on Google to establish the defense, to prove that express or implied consent actually exists as to the specific conduct at issue. But in evaluating the circumstances as a whole, it is clear users were not "explicitly" notified of the "specific practice" at issue. Instead, Google provided users conflicting information about personal data collection and use in the Chrome Privacy Notice and the general Privacy Policy.

Order Granting Google's Motion for Summary Judgment, Dkt. No. 935, 1-ER-9-10 [hereinafter "Order"]. Conflicting and insufficient disclosures did not explicitly notify a reasonable user of any "specific practice[s]." The surrounding circumstances only obscure implied consent further. The district court needed a 7.5 hour hearing and 8 witnesses to better understand the nature of the data collection at issue. *Id*. at 1-ER-17. Given the promises made in the Chrome Privacy Notice, a reasonable user could plausibly have interpreted Google's user agreement as not disclosing that it would collect and retain browser history of Chrome users. *See* In re Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019). Google therefore could not establish an affirmative defense of implied consent for a reasonable Chrome user.

Second, the district court's ruling rested on a flawed premise: that because *other* browsers transmit certain types of personal data to Google, Chrome users *also* consented to that transmission for their own browsing. Because the type of data collected by Google was "browser agnostic," the court reasoned that Chrome users had actually consented to the application of Google's more permissive "general policies"—not

Google's Chrome-specific privacy promises. Order, 1-ER-19. Put a different way: because the Safari browser shared the same kind of information with Google as Chrome did, Google was free to disregard the privacy protections it had advertised to Chrome users.

This is simply nonsensical, and it has no basis in contract law or consumer protection principles. How can a reasonable user possibly be held to this standard? The user would need to know the data collection and sharing practices of unrelated third parties in order to realize that the specific promises made in the Chrome Privacy Notice (or equivalent) would not protect their data. Moreover, the user would need to somehow know which alternate privacy policy and terms *would* control.

This model of consent would be flawed under any circumstance, but it is particularly implausible given the power and information asymmetry that characterizes Google's relationship with its users. Google's intricate knowledge of its own business practices, its vast array of services and data processing activities, and the panoply of complex user notices it publishes all conspire to make meaningful user consent a fiction. As detailed in Section III, the length, complexity, and numerosity of privacy policies today makes it "all but impossible for

users to fully comprehend what is done with their data." Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 Maine L. Rev 1, 30 (2022).[2] In the online ecosystem, "much of the data collection, data analysis, profiling, and behavioral targeting process remains unknown, incomprehensible, or unworkable to the average consumer." Peter J. van de Waerdt, *Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market*, Computer Law & Science Rev. (2020).[3] Even the best positioned consumer—one who has time to read privacy policies in full and toggle often-obscure privacy settings—still cannot meaningfully limit the collection and use of their personal information online because of the persistent asymmetry of information and power that platforms like Google enjoy.

Third, although the Court has determined the requirements for actual consent, it has not had occasion to resolve the precise issue in this case: whether a company can successfully raise an implied consent defense if its general disclaimer directly conflicts with other, specific promises the company made to the consumer. In other words, can a

[2] https://dl.acm.org/doi/pdf/10.1145/2976749.2978313.
[3] https://www.sciencedirect.com/science/article/pii/S0267364920300418.

reasonable person be presumed to have consented to general disclosures that conflict with specific promises? The Ninth Circuit should make clear that this scenario cannot support a finding of implied consent.

This result follows clearly from case law on the meaning of consent. For example, disclosures must only have "one plausible interpretation[.]" *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019). Additionally, consent can only be implied where the surrounding circumstances would indicate that a person knowingly agreed. *United States v. Staves*, 383 F.3d 977, 981 (9th Cir. 2004). The court could reach the same conclusion—that Google cannot establish the defense of implied consent—by analyzing either the surrounding circumstances or finding no "one plausible interpretation" of the conflicting Google policies. However the Court reaches this end result, the law should not enable Google, or any other company with similar practices, to continue disclaiming specific promises through conflicting general disclosures. This case, which highlights Google's misleading and extractive data practices, underscores why the law does—and should—require actual, meaningful consent. Google should not be able to disclaim its specific

privacy protections via contradictory terms in its general user agreement and ancillary disclosures. Affirming the ruling of the district court would represent a dangerous extension of the notice and choice privacy regime.

II. COURTS SHOULD RECOGNIZE THAT IMPLIED CONSENT MUST BE NARROW IN THE ONLINE PRIVACY CONTEXT TO PROTECT THE REASONALBE EXPECTATIONS OF USERS

In privacy law, there is a widely-shared concern that relying on a "reasonable person" standard to determine whether a given action violates an individual's right to privacy creates a circularity problem. *See* Lior Strahilevitz & Matthew Kugler, *The Myth of Fourth Amendment Circularity*, 84 U. Chi. L. Rev. 1747, 1757–59 (2017). The classic example of this problem in the Fourth Amendment context is positing that the government could eliminate a reasonable expectation of privacy merely by announcing that it would no longer respect it—that a certain type of surveillance would become commonplace and would thereby become constitutional. *See* Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 132–33 (2008) ("[T]he circularity problem [ ] afflicts expectations-of-privacy analysis. An announcement that all telephone calls will henceforth be monitored deprives people of their

reasonable expectations of privacy in such calls."). But ultimately courts do make normative determinations in privacy cases; the reasonable person standard is not meant to be an exercise in a detached, empirical analysis.

While the problem of circularity has been mostly a theoretical concern in Fourth Amendment law, it poses more fundamental problems in the area of consumer privacy law. Google and other internet companies have repeatedly violated consumer trust in their privacy practices over the last two decades, and their policies seem at times designed to lead users astray. Poll after poll shows that users expect and desire greater privacy protection online. But the invasive practices of internet companies and the skewed balance of power also leads to a sense of resignation. Users feel overwhelmed by the breadth of technical, legal, and commercial systems that are interwoven into the apps and websites that they use every day. And most users just want to access the internet in a safe and secure way, but they've been led to believe that is unattainable. *See* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, *Americans*

and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Rsch. Ctr. (Nov. 15, 2019).[4]

A court's role in determining whether a company should be able to assert the affirmative defense of consent in an online privacy case is about more than simply reviewing whether the company's privacy policy contains a disclosure that arguably describes the invasive conduct at issue. The court must evaluate what a reasonable user would understand given the full context: the nature of the service provided, the preferences and expectations of users of that service, and the promises and representations made by the company. Studies conducted over the last few decades have shown that users assumed privacy policies were drafted to solidify privacy protections; a majority of users polled would agree with the statement that "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users." Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, Pew Resch. Ctr. (Dec. 4, 2014).[5] So

[4] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[5] https://www.pewresearch.org/short-reads/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

in a case like this, where a company is alleged to have collected and retained sensitive browsing data after it represented that some users could limit the collection of that data, the Court should not assume that users agreed to generally disclaim their privacy interest in that sensitive data.

In addition to Google's express promise of heightened privacy protections, this Court should consider that Google exploits internet users' wish to not be tracked to trick them into believing that their data is not being collected. Courts have made clear that a company seeking to assert the affirmative consent defense bears the burden of showing that no reasonable user "could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct." *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019). When evaluating Google's disclosures from the perspective of the reasonable user, it is essential to take into account Google's privacy promises in response to users' demands for greater privacy online and the fact that courts have found that the Terms of Service and Privacy Policies are used to "obscure Google's intent to engage" in invasive conduct. 2021 Order

Granting in Part and Denying in Part Motion to Dismiss with Leave to Amend, Dkt. No. 142, 3-ER-408 (citing *In re Google, Inc.*, 2013 WL 5423918, slip op. at *13 (N.D. Cal. Sept. 26, 2013)). People do not wish to be tracked online. Google knows this. Google exploits this. This is why Google presented a misleading promise to its users that it would protect their privacy.

The lower court's decision implied that whether Google obtained actual consent does not matter because other third-party browsers would have shared similar information with Google. This discussion is both irrelevant and an incorrect way to frame the issue. The question before the court is whether a reasonable user would understand all of Google's statements, promises, and conduct to mean that it will collect data that it expressly promises it would not, regardless of how Google interacts with, or collects data from, third parties. Internet users deserve the protections that they are promised. The lower court's decision says those promises are meaningless.

When presented with a meaningful choice to limit online tracking, people will generally choose to protect their privacy. Take Apple's App Tracking Transparency initiative, which gave Apple users control over

their unique serial number for their devices, also known as the identifier for advertisers ("IDFA"). Sara Morrison, *The Winners and Losers of Apple's Anti-Tracking Feature*, Vox (Apr. 29, 2022).[6] This identifier allows trackers to recognize a device across different apps so that they can link app activity to a person's specific device. Apple's App Tracking Transparency initiative prevented a user's IDFA from being surveilled by advertisers unless the user opted into such tracking. In the weeks following the rollout of ATT, one analyst determined that only 5% of U.S. Apple users consented to such cross-app tracking. Estelle Laziuk, *iOS 14.5 Opt-in Rate – Daily Updates Since Launch*, Flurry (May 25, 2021).[7] In the years since the majority of users—numbering in the hundreds of millions—have chosen to decline tracking by opting out. Morrison, *supra*; Konrad Kollnig et al., *Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy*

[6] https://www.vox.com/recode/23045136/apple-app-tracking-transparency-privacy-ads.
[7] https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

Labels, 2022 ACM Conference on Fairness, Accountability, and Transparency 508–20.[8]

Google's "consent" practices are especially troubling: its misleading and conflicting privacy policies contradict user intention because internet users do not wish to be tracked online and will choose a privacy protective option when presented with a choice. Knowing this, Google leads a reasonable user into believing that they are in control of their privacy when they are not. While promising users heightened specific privacy protections because Google knows users want them, Google is able to collect excessive user data in contravention of what users expect because of these very promises.

The court should assume that Chrome users reasonably expect, at a minimum, that Google will not collect and make available *more* private browsing data from them than it does from users of other browsers. But the record shows that Google provides browsing data from Chrome users that is connected to a special unique identifier. *See* Order Granting Google's Motion for Summary Judgment, Dkt. No. 935,

[8] https://doi.org/10.1145/3531146.3533116 ("Preliminary data suggests that the vast majority of users (between 60% and 95%) choose to refuse tracking when asked for it under the new system[.]").

1-ER-18-19. So even if the lower court's conclusion were correct that Chrome users consented to some amount of data collection about their browsing activity, Google's collection and linking of user data nevertheless exceeds what a reasonable user would expect based on the company's disclosures. A reasonable user would likely understand that *some* data collection, storage, and retention is necessary for the functionality of the browser. But if a user chooses a privacy-protective option to limit the collection and linking of their personal information, that user would expect the scope of the collection and use of their personal information to be limited accordingly to reflect that choice. The district court's decision defies this reasonable consumer expectation.

If this Court embraces the expansive view of disclosure-based express consent presented by Google in this case, companies will be incentivized to disclose broad data collect permissions and further erode consumers' feeling of control over their personal information online. Surveys show that Americans would like to control the data that companies have about them but do not believe that they can attain that level of control on their own. Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting*

American Consumers and Opening Them Up to Exploitation (June 26, 2015).[9] This privacy resignation (or digital resignation) "occurs when a person believes an undesirable outcome is inevitable but feels powerless to stop it." *Id.* at 3. Recent research about privacy resignation "definitively negates the idea that Americans feel that they can adequately understand and consent to marketers' data-gathering regime."[10] Joseph Turow et al., *Americans Can't Consent to Companies' Use of Their Data*, Annenberg School for Communication, University of Pennsylvania 6 (2023). One study found that 91% of Americans want to have control over what marketers can learn about them online but 79% of Americans believe that they have little control over this practice.[11] *Id.* at 15. Further, most Americans believe that marketers' use of their

[9] https://ssrn.com/abstract=2820060.
[10] https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.
[11] "When we investigated the overlap that designates resignation, we found that a large majority of the population—74%—is resigned. They believe they live in a world where marketers taking and using their data is inevitable."

personal information can harm them but are resigned to their powerlessness. *Id.* at 16.[12]

Consumers do not wish to give up their personal information but believe it is inevitable when they do not have any control over it. Data practices such as Google's in this case are the very reason that consumers feel resigned. Even when consumers believe that they can limit certain uses of information, companies like Google prevent this. That is why this Court must take user preferences into account when evaluating both the existence and scope of affirmative consent from the perspective of the reasonable user.

III. CONSUMERS CANNOT HAVE MEANINGFUL CHOICE IF COMPANIES CAN ASSERT A DEFENSE TO PRIVACY CLAIMS WHEN THEIR GENERAL DISCLAIMERS CONTRADICT SPECIFIC PROMISES

For more than two decades, Google and other companies online have sought to frame their privacy practices in terms of user "choice." Their policies and terms of service, so the argument goes, provide users

[12] "Fully 80% of the population agrees that what companies know about them from their online behaviors can hurt them. Moreover, 62% of Americans believe they can be harmed and are resigned. Put differently, about 6 in 10 Americans believe that what companies know about them can hurt them, and that they are powerless to stop it."

with "notice" of their practices, and then present those users with a choice about what do with their data. But the only real "choice" most users have is to accept these policies and practices blindly or to refrain from using the service. The Federal Trade Commission, and many other regulators and oversight bodies, recognized from the early days of the modern internet that this system did not provide meaningful notice or meaningful choice because few users had the time or wherewithal to parse these dense and confusing policies. Fed. Trade Comm'n, *Self-Regulation and Privacy Online: A Report to Congress* 4 (July 1999).[13]

Even though terms of service and policies do not provide users with meaningful notice or choice regarding a provider's privacy practices, they have been used by companies to support the affirmative consent defense and to undercut merits arguments in some privacy cases. *See Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018). But the question in those cases was whether consent could be implied based on the disclosures contained in a company's general privacy policies or terms of service. *Id.* This case presents a very different question, which

[13] https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf

is whether a company's express promise to protect the privacy of certain data for certain users changes the analysis of implied consent. This Court should hold that it does—or else users will lose any ability to meaningfully evaluate online apps and services to protect their privacy.

Google has argued in this case that an individual's "agreement" to their Privacy Policy and Google Account Holder agreements means that they consent to all potential data collection described not only in the policies and agreements, but also in any other linked disclosures, FAQs, and other documents. *See* Google's Motion for Summary Judgment Dkt. No. 395 at 14–16 [hereinafter Google MSJ]. But at the same time Google argues that the more specific representations made in its Chrome Privacy Notice are irrelevant because those disclosures relate to "features that are specific to Chrome." *Id.* at 18. Under this view, users can never trust a specific privacy promise made by a company like Google because that promise could be qualified, disclaimed, or contradicted in the fine print elsewhere. Heads they win, tails users lose. The Court should reject this argument.

This case presents a quintessential example of how the "notice and choice" approach is used to undermine user privacy at every turn.

Notice and choice has never been about seeking the actual consent of users or about protecting their privacy. *See* Samuel Levine, Dir. Bureau of Consumer Prot., Fed. Trade Comm'n, *Remarks at the 2023 Consumer Data Industry Association Law & Industry Conference: Surveillance in the Shadows Third-Party Data Aggregation and the Threat to our Liberties* 2 (Sept. 21, 2023).[14] The notice and choice regime has made privacy self-management impracticable while emboldening the expansion of commercial surveillance systems and incentivizing the continuous extractions of consumer data. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1879, 1885–86 (2013). This problem is further exacerbated by the extreme information asymmetries between a single user and an enormous, powerful company; in these circumstances consumers have at best an illusory sense of control without the meaningful choice to negotiate terms other than to opt out of the digital economy entirely.

This section will consider the history of the notice and choice regime, analyze the systemic failures these systems have fueled to

[14] https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf.

undermine the agency of internet users, and explain why the actual purpose of notice and choice has been to enable the boundless consumer data collection.

A. Notice And Choice Has Overstayed Its Welcome And Failed To Secure Meaningful Consent For Consumers

In the early age of computers and the internet, the notice and choice paradigm emerged to address individual rights related to basic data collection. The concept was twofold: a data collector discloses the purpose and use of the information it plans to collect, and individuals consider whether to decline or consent to allow their data to be collected. This notice and choice paradigm appeared as a privacy principle in the foundational 1973 *Records, Computers and the Rights of Citizens* report, which advocated for Congress to adopt the Fair Information Practices. Secretary's Advisory Committee on Automated Personal Data Systems., U.S. Department of Health, Education. & Welfare, *Records, Computers, and the Rights of Citizens* 41–42 (1973). It was then incorporated into the Privacy Act of 1974, which requires government agencies to provide notice of privacy practices and obtain consent from individuals to enable disclosure of information. 5 U.S.C. § 552(a). On a global stage, the Organisation for Economic Co-operation

and Development similarly endorsed a notice and choice framework in its 1980 "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Org. for Econ. Coop. and Dev., *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD (Sept. 23, 1980).

In practice, notice and choice has not been an effective mechanism to protect consumer privacy. Rather, the failure of notice and choice to provide consumers with the ability to meaningfully consent to data collection and use has been foundational to the growth of the commercial surveillance system. In the absence of adequate federal data protection standards, consumers are unreasonably expected to self-manage their privacy as online firms "deploy commercial surveillance systems that collect and commodify every bit of our personal data." EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 7 (Nov. 2022).[15] The "fiction of notice and choice," has ushered in an era of commercial surveillance that ironically strips consumers of their autonomy while exposing

[15] https://epic.org/documents/disrupting-data-abuse-protecting-consumers-from-commercial-surveillance-in-the-online-ecosystem/.

consumers to data privacy and data security risks. Levine, *supra*, at 2. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. Online 793, 849 (2021).

B. The Notice And Choice Regime Prevents Actual Consent

The problems related to notice and choice are "both widespread and well documented." World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction* 7 (July 2020).[16] First, the "notice" provided to a consumer takes the form of dense, incomprehensible, and extremely long disclosures. "Privacy policies run for thousands of words and are generally not designed to optimize consumer understanding." Lancieri, *supra*, at 29. Even if a consumer tried, many data collection practices "are too complex and numerous for even the most sophisticated consumer to understand." EPIC, *supra*, at 3.

Next, the illusory "choice" to accept the terms of the privacy disclosure is not meaningful consent. There is no room for negotiation or

16 https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf.

actual choice, and it is not realistic for consumers to withdraw from the online world. *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online*, 66 Clev. St. L. Rev. 559, 559 (2018) [hereinafter "*Against Notice and Choice"*]. Information and power asymmetry persists through the entire transaction: the consumer remains uninformed or underinformed by design, as the "data collection, data analysis, profiling, and behavioral targeting process remains unknown, incomprehensible or unworkable to the average consumers." Peter J. van de Waerdt, *Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market*, 38 Computer Law & Security Rev. 1, 2 (2022).

1. Privacy Self-Management is Impracticable

Privacy disclosures are opaque, lengthy, and vague. Even if a consumer had the unlimited time and patience to read each privacy policy, they likely would not understand the consequences of accepting the terms disclosed in the notice. Lancieri, *supra*, at 30. A recent University of Pennsylvania study found that "overwhelmingly, and to an extent not known before, Americans neither understand commercial surveillance practices and policies nor do they feel capable of doing

anything about rampant data extraction." Turow, *Americans Can't Consent*, *supra*, at 17. Notice and choice amounts to blanket consent to every policy outlined in a privacy disclosure, even if it is "impossible for users to fully comprehend what is done with their data." Lancieri, *supra*, at 30.

Privacy self-management through notice and consent also faces structural problems, leaving people without the ability to have meaningful control over their data. *See* Solove, *supra*, at 1888, 1893. The sense of control provided by clicking "I accept" is illusory because the complexity and power of digital networks makes individual control impossible, as technology companies "rely on a click-to-agree button to give them permission to do whatever they want with user data." Turow, *Americans Can't Consent*, *supra*, at 6. A single user is too overwhelmed by so many entities simultaneously collecting and using their data every day for realistic privacy self-management, and undisclosed privacy harms can result from the aggregation or consolidation of data by those different entities. *See* Shara Monteleone, *Addressing the "Failure" of Informed Consent in Online Data Protection: Learning the*

Lessons From Behaviour-Aware Regulation, 43 Syracuse J. Int'l L. & Com. 70, 89–90 (2015).

Privacy policies cannot effectively disclose the risks from data collected and shared with third parties, or from future, unnamed secondary uses of that data. Against Notice and Choice, *supra*, at 634; *see* EPIC, *supra*, at 159; Solove, *supra*, at 1983. "The emphasis on setting the rules at the point of collection of the data fails to take account of the reality of the value of business-to-business sharing of personal data," because once the data "enters the value chain," seeking reconsent for future transactions or unforeseen uses of data becomes challenging. World Economic Forum, *supra*, at 11. Despite the illusion of control, the compounding problems of scale, aggregation and the inability to assess future harm make privacy self-management through notice and choice unrealistic.

2. Notice and Choice Maintains Unfair, Extractive Data Practices

Data collection, accumulation, and aggregation is lucrative, and the data-fueled market continues to grow rapidly. The data aggregator industry is estimated to top $450 billion in the next ten years. Levine, *supra*, at 4-5. "Consumer-facing firms are incentivized to extract as

much data as they can, while the third parties involved are incentivized to find new ways to monetize it[.]". *Id*. at 5. Notice and choice has proven to be a frictionless mechanism for unhindered data collection. *See* World Economic Forum, *supra*, at 9. Businesses can extract and use seemingly unlimited amounts of data relying nefariously on consumer resignation to agree to lengthy, incomprehensible privacy policies. As a result, consumers do not have the ability to "select a product that offers noticeably better protection of their personal information," because there is no competition or incentive for better privacy policies to develop. John A. Rothschild, *Sham Choice: How the Current Privacy Regime Fails Us and How to Fix It*, 92 UMKC L. Rev. 169, 198 (2023).

In a general sense, the notice and choice interaction between business and consumer involves two transactions related to personal information. *Id*. at 172. First, the parties agree that the business will provide a service and the consumer will divulge personal data for that purpose. The second transaction involves "the business's proposal that it be allowed to collect additional personal information or to use the consumer's information for purposes extraneous to the provision of the good or service." *Id*. This second transaction likely has nothing to do

with the first transaction but enables the seller to monetize the consumer data further. If the consumer wants to continue with the transaction, the notice and choice regime does not provide them with the right or opportunity to reject the seller's secondary use or additional collection of personal information. *Id.* at 184. "The absence of such choice means that a privacy regime premised on notice and choice […] acts as a cover for a system that presents consumers with no privacy choices at all." *Id.* at 198.

Through this historical lens, this Court should understand that the notice and choice regime has failed users. Despite users' desire to be tracked less, this regime has continued to erode users' privacy online while companies have capitalized on extensive data collection. Relying on notice and choice has led to a broken system of "consent" in 2023 where a company like Google can attempt to assert consent as an affirmative defense to a privacy claim by providing a general disclosure that contradicts specific privacy promises made to users. No reasonable user can actually consent to the collection of their personal information when a single general disclosure can undermine specific protections promised to them. A decision that does not find for Plaintiff-Appellants

will affirm and extend the extractive, unfair nature of the notice and choice regime that prevents actual consent.

CONCLUSION

For the foregoing reasons, *amicus* respectfully urges the Court to reverse the district court's order granting Defendant's Motion for Summary Judgment.

Date: December 21, 2023

/s/ Alan Butler
Alan Butler
Sara Geoghegan
Suzanne Bernstein
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 6,293 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

[ ] it is a joint brief submitted by separately represented parties;

[ ] a party or parties are filing a single brief in response to multiple briefs; or

[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: */s/ Alan Butler* **Date:** December 21, 2023

CERTIFICATE OF SERVICE

I certify that on December 21, 2023, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: December 21, 2023

/s/ Alan Butler
Alan Butler
Sara Geoghegan
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center