NO. 22-16993

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

PATRICK CALHOUN, ET AL., on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

v.

GOOGLE LLC,

Defendant-Appellee.

On Appeal from the United States District Court for the Northern District of California (Case No. 20-cv-5146) (District Judge Yvonne Gonzalez Rogers)

BRIEF OF WASHINGTON LEGAL FOUNDATION AS AMICUS CURIAE SUPPORTING DEFENDANT-APPELLEE AND AFFIRMANCE

Cory L. Andrews
John M. Masslon II
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Ave. NW
Washington, DC 20036
(202) 588-0302
candrews@wlf.org

February 15, 2024

RULE 26.1 DISCLOSURE STATEMENT

Washington Legal Foundation has no parent company, issues no stock, and no publicly held company owns a ten percent or greater interest in it.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(*continued*)

Statute

Other Authorities

TABLE OF AUTHORITIES
(*continued*)

INTEREST OF AMICUS CURIAE*

Washington Legal Foundation is a nonprofit, public-interest law firm and policy center with supporters nationwide. WLF promotes free enterprise, individual rights, limited government, and the rule of law. It often appears before this Court as an amicus curiae to oppose novel theories of civil liability that would unduly hinder investment and innovation in the digital economy. *See, e.g., Epic Games, Inc. v. Apple, Inc.*, 67 F.4th 946 (9th Cir. 2023); *Facebook, Inc. v. Patel*, 932 F.3d 1264 (9th Cir. 2019).

INTRODUCTION

No one disputes that safeguarding the privacy of internet users is critical. That is why Google scrupulously discloses its data-retention policies and practices to its users. Google's Privacy Policy and other agreements clarify, in plain language that is easy to follow, that Google receives data whenever users of *any* browser visit third-party websites that have installed Google Ads, Google Analytics, and other Google web services. Plaintiffs here viewed these disclosures and clicked "I AGREE"

* No party's counsel authored any part of this brief. No one, apart from WLF and its counsel, contributed money intended to fund the brief's preparation or submission. All parties consented to WLF's filing this brief.

to their terms. When they clicked "I AGREE," Plaintiffs knowingly consented to Google's data-retention practices. And under long settled law, Plaintiffs may not recover for conduct to which they have knowingly consented.

Yet despite their unambiguous consent to Google's data-collection policies and practices, Plaintiffs implausibly claim that they were caught unaware by the very policies and practices they agreed to. They point instead to a separate, unrelated privacy notice for Google's web browser—Google Chrome. Relying on unique features "specific to Chrome," Plaintiffs purportedly assumed that disabling Chrome's "Sync" feature—which allows users to enjoy the same Chrome browser settings and preferences across multiple devices—would somehow prevent Google from receiving data on third-party websites that use Google's web services. The District Court rightly saw through this distortion of the plain text and meaning of the disclosures and entered summary judgment for Google.

That judgment should be affirmed. Web-service providers like Google should not face liability from post-hoc, phantom "promises" cobbled together from snippets of disparate, unrelated notices. To disclose data-retention practices effectively, web-service providers must remain free to write general, easy to understand policies that describe their collection of

user-generated data in a way that users are likely to read and understand. *See, e.g., Smith v. Facebook, Inc.*, 745 F. App'x 8, 8–9 (9th Cir. 2018) (finding that a broad, general disclosure is sufficient).

Plaintiffs' approach, in contrast, would create perverse incentives for exhaustive disclosures that overwhelm users with too much information. That would defeat the very point of disclosure—informed consent. Allowing Plaintiffs to proceed to trial would also inject massive uncertainty into tech companies' litigation exposure, which would no doubt chill investment in innovative products and services. Plaintiffs' bizarre approach to consent, if embraced on appeal, would ultimately harm consumers, businesses, and the American economy.

STATEMENT

Google offers web services—like Ads, Analytics, Maps, and Fonts—to third-party websites seeking to monetize their content or enhance their functionality. (7-ER-1380–82) Google receives data whenever users visit—in *any* browser—websites that have installed these services, which Google uses to route content to the correct IP address, optimize content for users' devices, provide insights to publishers, target ads, and improve its services. (2-ER-178, 195–96, 199; 7-ER-1380–82) Google fully discloses this data collection and use in its general Privacy Policy. (7-ER-1379 ¶ 51)

Separately and unrelatedly, Google also offers Chrome, Google's free web browser. Chrome offers a "Sync" feature, which allows users to store Chrome browser information—like bookmarks, passwords, settings, and history—so that users may enjoy the same Chrome experience across devices. (7-ER-1350–51) Google describes Sync in its Chrome Privacy Notice, which details "features that are specific to Chrome." (3-ER-357) It explains that "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." (3-ER-409–10)

Plaintiffs here are Chrome users who chose not to use Sync. They allege breach of contract, tort, and statutory claims against Google because Google received data when Plaintiffs browsed on websites that used Google's third-party web services. It is undisputed that Google did not receive the at-issue data through Sync. Even so, Plaintiffs contend that Google was prohibited from collecting that data unless users enabled Sync, an unrelated Chrome-specific feature.

Following robust briefing and an all-day evidentiary hearing with testimony from eight witnesses, the District Court granted summary judgment to Google and held that Plaintiffs consented to Google's receipt and use of all at-issue data when they agreed to the Privacy Policy and

Account Holder Agreements. Because the challenged data collection occurred regardless of browser, the District Court determined that Google's Privacy Policy and Account Holder Agreements, not the Chrome-specific notice, resolve this case. All Plaintiffs expressly agreed to the Privacy Policy and Account Holder Agreements, which adequately disclosed Google's at-issue data collection.

On appeal, Plaintiffs argue that Google's Chrome-specific disclosures somehow negated their clear consent to the Privacy Policy's and Account Holder Agreements' data-collection practices, which apply to all users across *all* browsers.

SUMMARY OF ARGUMENT

I. Plaintiffs (at 4) accuse the District Court of adopting "a novel consent framework." But no principle of law is better settled than *volenti non fit injuria*, "no wrong is done to one who consents." Simply put, a party may not complain of conduct to which it has consented. There is nothing "novel" about this venerable rule, which California has adhered to for more than a century and a half. *See* Cal. Civ. Code § 3515 (1872). This affirmative defense, which the District Court rightly found covers all of Plaintiffs' claims here, easily resolves this appeal. Because each Plaintiff

expressly and knowingly consented to Google's receipt and use of at-issue data, the District Court's judgment should be affirmed.

II. Allowing Plaintiffs to impose liability on Google for data retention practices to which they've knowingly consented would invite disastrous, unintended consequences. Plaintiffs' position, if adopted, would create runaway liability risks for virtually any data disclosure. In such a litigious climate, companies seeking to avoid liability would doubtless resort to overdisclosure, which imposes unnecessary costs and burdens on businesses and consumers alike. That is not an outcome this Court should welcome.

III. Innovation in the technology sector has been an enormous boon to the U.S. economy. Many wonderful web-based products and services are free, thanks to targeted advertising—and thanks to the conventions for disclosure and consent on which Google and others have come to rely. Yet if internet-based businesses face an onslaught of privacy litigation, they may have to stop offering these innovative products and services to avoid liability exposure. If American consumers and companies lose access to these innovations, the United States would become a laggard in this fast-growing sector of the global economy. That would be a calamity.

ARGUMENT

I. PLAINTIFFS SHOULD NOT RECOVER FOR CONDUCT TO WHICH THEY KNOWINGLY CONSENTED.

Rather than embracing "a novel consent framework," as Plaintiffs suggest (at 4), the District Court's conclusion that Plaintiffs' consent is a complete defense to their claims is confirmed by state and federal caselaw, the Restatement of Torts, learned treatises, and longstanding public-policy considerations. Because each Plaintiff expressly consented to Google's receipt and use of all at-issue data, the District Court's judgment should be affirmed.

A party is not remotely harmed by conduct to which it has consented. *Volenti non fit injuria*, "no wrong is done to one who consents," is a rule of law so venerable that it predates the common law itself. In fact, for about as long as there have been civil trials, plaintiffs have been precluded from obtaining relief for conduct to which they have consented. While consent as a legal defense first appeared in English common law in 1304, the concept has origins in classical antiquity. *See* Terence Ingman, *A History of the Defence of* Volenti Non Fit Injuria, 26 Jurid. Rev. 1, 1–3 (1981) (tracing the concept to Aristotle's *Nicomachean Ethics* and Justinian's *Codex*).

Consent is a cornerstone of modern tort law. *See*, *e.g.*, William Prosser, *Prosser on Torts* 101, § 18 (4th ed. 1971) ("It is a fundamental principle of the common law that *volenti non fit injuria*, to one who is willing, no wrong is done."); Restatement (Second) of Torts § 892A (1979) ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or harm resulting from it."); *Black's Law Dictionary* 1605 (8th ed. 2004) ("[T]o a willing person it is not wrong."). Alleged privacy torts are no exception. *See* 77 C.J.S., Right of Privacy, § 6 (1978) ("The right of privacy may be waived by the individual or by anyone authorized by him, and this waiver may be either express or implied.").

Consent enables free enterprise and fosters harmony. "The power to consent enlarges personal freedom, autonomy, and agency, while also facilitating mutually beneficial relationships and transactions between people." Restatement (Third) of Torts § 12 cmt. c (Am. Law Inst., Tentative Draft No. 4, 2019). As one scholar has put it, "consent turns a trespass into a dinner party; a battery into a handshake; a theft into a gift; an invasion of privacy into an intimate moment; a commercial appropriation of name and likeness into a biography." Heida M. Hurd, *The Moral Magic of Consent*, 2 Legal Theory 121, 123 (1996).

No surprise, then, that since 1872 California law has insisted that one "who consents to an act is not wronged by it." Cal. Civ. Code § 3515 (1872); *Churchill v. Bauman*, 82 P. 979 (Cal. App. 1892) ("It is a general rule of the English law that no one can maintain an action for a wrong where he has consented to the act which occasions his loss."). And California law has long denied relief to plaintiffs alleging privacy harms when those plaintiffs consented to the alleged conduct. *See Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 623, 657 (Cal. 1994) (applying the defense of consent to invasion of privacy claims where plaintiff agreed to the alleged invasion).

Indeed, California courts have consistently held that plaintiffs who voluntarily consent to sharing their data cannot turn around and seek recovery for invasion of privacy. *See, e.g., TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal. App. 4th 443, 452–53 (2002) (company's notice to plaintiff, in the form of a policy, coupled with plaintiff's written consent to the policy, defeated plaintiff's privacy claim); *Feminist Women's Health Ctr. v. Superior Court*, 52 Cal. App. 4th 1234, 1247–49 (1997) (plaintiff's consent to even a serious invasion of privacy defeated the plaintiff's claim of a reasonable expectation of privacy). This case is no different.

Given Google's explicit disclosure that it receives and uses Plaintiffs' at-issue data *no matter the browser*, combined with Plaintiffs' clicking "I AGREE" to disclosures that accurately described the very conduct in question, no Plaintiff could have an expectation of privacy that Google violated here. "When one clicks 'I agree' to the terms on the box, does one usually know what one is doing? Absolutely. There is no doubt whatsoever that one is objectively manifesting one's assent to the terms in the box, whether or not one has read them." Randy E. Barnett, *Consenting to Form Contracts*, 71 Fordham L. Rev. 627, 635 (2002). In California (as elsewhere), such voluntary consent precludes recovery. *Hill*, 865 P.2d at 648 ("If voluntary consent is present, a defendant's conduct will rarely be deemed 'highly offensive to a reasonable person' so as to justify tort liability.") (citing Restatement (Second) of Torts, § 652B, cmt. c).

And there is simply no way that Google's industry-standard commercial activity rises to the level of "highly offensive" conduct that courts require to plead a common-law privacy claim. *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1082 (Cal. App. 2009) (finding that a workplace surveillance system, even though hidden from employees, was not highly offensive and prompted by legitimate business concerns). No reasonable user would believe that disabling Sync—a feature that applies

only to Google Chrome—would somehow limit the data shared on third-party websites that have installed Google Ads, Google Analytics, and other Google web services.

Here, the District Court granted summary judgment for Google after a full-day evidentiary hearing with eight witnesses—three experts and five fact witnesses. Even after drawing all reasonable inferences in Plaintiffs' favor, the District Court concluded that the uncontested evidence showed that Plaintiffs consented to Google's receipt of all at-issue data when they agreed to the Privacy Policy and Account Holder Agreements. This Court has reached the same conclusion in a nearly identical case. *See Smith v. Facebook, Inc.*, 745 F. App'x at 8–9.

In sum, consent is a complete defense here. Plaintiffs' knowing and voluntary consent to Google's receipt and use of their at-issue data renders their claims meritless. See *Hill*, 865 P.2d at 648 ("The maxim of the law '*volenti non fit injuria*' (no wrong is done to one who consents) applies as well to the invasion of privacy tort.") Allowing Plaintiffs to recover for conduct to which they knowingly consented would not only be unfair to Google, it also would upend tort liability and invite a torrent of speculative strike suits.

II. ALLOWING BOUNDLESS LIABILITY FOR UNAMBIGUOUS PRIVACY DISCLOSURES WOULD INVITE OVERDISCLOSURE AND UNDERMINE INFORMED CONSENT.

Plaintiffs' position, if adopted, would create outsized litigation risks for any company that fails to bury its users in an avalanche of data-retention policy minutiae. Yet many privacy critics already contend that data privacy disclosures are far too long to be effective. When a tech pundit recently tallied up all the privacy notices for his phone's apps, they totaled nearly a million words—twice as long as Tolstoy's *War and Peace*. *See* Geoffrey A. Fowler, *I tried to read all my app privacy policies. It was 1 million words*, Wash. Post, May 31, 2022, https://perma.cc/NP8T-3HRS.

Scholars have long warned against bloated disclosures that bury useful information under an avalanche of irrelevant and distracting words. The danger is that "consumers may be inundated with so many pieces of information that they cannot process all the . . . messages they receive." W. Kip Viscusi, *Individual Rationality, Hazard Warnings, and the Foundations of Tort Law*, 48 Rutgers L. Rev. 625, 633 (1996); *see also* Troy A. Paredes, *Blinded by the Light: Information Overload and its Consequences for Securities Regulation*, 81 Wash. U.L.Q. 417, 419 (2003) ("Studies show that at some point, people become overloaded with information and make worse decisions than if less information were made

available to them."); Howard Latin, *"'Good' Warnings, Bad Products, and Cognitive Limitations*, 41 UCLA L. Rev. 1193, 1212 (1994) (emphasizing that "'too much' information can be just as much of an impediment to effective user comprehension . . . as 'too little' knowledge would be").

The result of *over*disclosure is often the same as nondisclosure, as genuinely useful information becomes hidden in plain sight. "[T]he more information there is, the more each bit of it is diluted. The immediate and salient crowds out the less attention-grabbing." Donald C. Langevoort, *Toward More Effective Risk Disclosure for Technology-Enhanced Investing*, 75 Wash. U. L.Q. 753, 759 (1997) (footnote omitted). Because of this "information overload," a "large amount of information" can become "equivalent to no information at all." Cass R. Sunstein, *Informing America: Risk, Disclosure, and the First Amendment*, 20 Fla. St. U. L. Rev. 653, 668 (1993).

The problem of overdisclosure is thus well recognized in the law and literature concerning product manufacturers' duty to warn consumers about product risks. "The inclusion of each extra item dilutes the punch of every other item. Given short attention spans, items crowd each other out; they get lost in fine print." *Cotton v. Buckeye Gas Prods. Co.*, 840 F.2d 935, 937–38 (D.C. Cir. 1998); *see Robinson v. McNeil Consumer Healthcare*,

2010 WL 3156548, at *7 (7th Cir. Aug. 11, 2010) ("[I]nformation overload would make label warnings worthless to consumers."). The Supreme Court has long recognized this basic truth of human psychology: "*Meaningful* disclosure does not mean *more* disclosure." *Ford Motor Credit Co. v. Milhollin*, 444 U.S. 555, 568 (1980); *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 448–49 (1976) ("[A]n avalanche of trivial information . . . is hardly conducive to informed decisionmaking.").

Federal regulators too have cautioned against the perils of informational overload. The Food and Drug Administration, for instance, has concluded that overdisclosure "can cause meaningful risk information to 'lose its significance.'" 71 Fed. Reg. 3922, 3935 (Jan. 24, 2006). "Overwarning, just like underwarning, can similarly have a negative effect on patient safety and public health." *Id.* The Securities and Exchange Commission has likewise urged public companies to avoid "unnecessary duplicative disclosure that can tend to overwhelm readers" and to "focus on material information and eliminate immaterial information that does not promote understanding of companies' financial condition." 68 Fed. Reg. 75056, 75057 (Dec. 29, 2003).

Effective disclosure thus requires a sensible balance between competing considerations of completeness and the need to avoid

informational overload. Yet even the *risk* of liability can create hydraulic pressure for more exhaustive disclosures. Such overdisclosure does more than just make the average disclosure longer. In the case of data privacy, overdisclosure runs contrary to the very purpose of disclosure—ensuring informed consumer consent.

In short, adopting Plaintiffs' position would create outsized litigation risks incentivizing companies to disclose every exhaustive detail of data collection and use, which would make disclosures less clear and less likely to be read. Such disclosures would erode informed consent. That would benefit no one.

III. PLAINTIFFS' APPROACH TO PRIVACY LIABILITY WOULD CREATE UNCERTAINTY AND STIFLE INNOVATION.

Businesses "crave certainty as much as almost anything: certainty is what allows them to make long-term plans and long-term investments." Alan Greenspan & Adrian Wooldridge, *Capitalism in America: A History* 258 (2018). Web-service providers and other internet-based businesses need clear rules of the road to continue offering innovative products and services. Plaintiffs' approach to consent injects great uncertainty into the technology sector. That uncertainty will stifle innovation, as companies could not update a product's features or default settings without

drastically overhauling their disclosures. And even then, there would be no guarantee that the new disclosures would protect the company from liability.

Nor is that all. Particularly when styled as class actions, lawsuits can exert hydraulic leverage on defendants to settle even unmeritorious claims. "With vanishingly rare exception, class certification sets the litigation on a path toward resolution by way of settlement, not full-fledged testing of the plaintiffs' case by trial." Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. Rev. 97, 99 (2009). As the Supreme Court has recognized, "extensive discovery and the potential for uncertainty and disruption in a lawsuit allow plaintiffs with weak claims to extort settlements from innocent companies." *Stoneridge Inv. Partners, LLC v. Scientific-Atlanta*, 552 U.S. 148, 163 (2008) (citing *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 740–41 (1975)).

This increased threat of tort liability has the potential not only to distract innovative firms, reducing the quality of innovation, but also to raise the cost of innovation, thus reducing the quantity. *See* Peter W. Huber, *Liability: The Legal Revolution and Its Consequences* 1–3 (1988) (showing how the dramatic increase in tort litigation puts American businesses at a global competitive disadvantage). This is no small matter.

Virtually every brick-and-mortar business in the United States, from the smallest mom-and-pop shop to the largest multi-national corporation, maintains an internet website. According to the Bureau of Economic Analysis (BEA), America's "digital economy" accounted for $2.6 trillion of GDP in 2022. *See* U.S. Bureau of Economic Analysis, *How Big Is the Digital Economy?* (Dec. 6, 2023), http://tinyurl.com/2ej5pav2. That investment—which comprised ten percent of U.S. GDP—accounted for 8.9 million jobs and $1.3 trillion in compensation. *Id.*

Studies have shown that abusive privacy-tort litigation increases costs for businesses while providing little in the way of redress for consumers, improved privacy practices, or deterrence. "[L]itigation is especially problematic in the privacy context, as it undermines appropriate agency enforcement, clutters the courts, and chills innovation and nationwide service deployment." Mark Brennan, *Ill-Suited: Private Rights of Action and Privacy Claims* 1 (Institute for Legal Reform, 2019), https://perma.cc/6BXT-E7MD. Such lawsuits "hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies." *Id.* at 14.

Take targeted online advertising, which provides clear benefits to both consumers and competition. Plaintiffs' view of consent, if embraced on appeal, would create a tort climate in which targeted advertising is no longer economically feasible. That would be a net loss for consumers. Many wonderful products and services are free, thanks to advertising—and thanks to the conventions for disclosure and consent on which Google and others rely. Targeted ads thus benefit consumers by providing more relevant ads and, in many cases, supporting access to free services that consumers may otherwise have to pay for. As the Federal Trade Commission has explained, targeted advertising "benefits the consumer because it effectively reduces their search costs." Federal Trade Commission, Yan Lau, *A Brief Primer on the Economics of Targeted Advertising* 5 (Jan. 2020), https://perma.cc/G8F5-NRU6. Ad targeting can also "mean fewer ads overall; consumers benefit directly from not having to view ads, but also indirectly from cost-savings passed on by firms." *Id.* at 12.

What's more, targeted ads benefit competition by making it more cost efficient for small businesses to engage in advertising and to maximize their smaller marketing budgets. Indeed, by reducing search costs and improving match quality, targeted ads help "increase price

competition," which "increases the total value consumers derive from acquiring the products they match with." *Id.* In contrast, depriving U.S. consumers and businesses of access to new and emerging web-based technologies would make America a laggard in adopting those technologies.

Ongoing investment in the vital tech sector requires a stable and predictable legal regime that protects investment by enabling innovative firms to avoid limitless liability. Allowing Plaintiffs to recover for routine data collection and everyday internet-marketing practices to which they've knowingly consented would send shockwaves across the digital economy. This threat of unpredictable liability—in the face of a user's unambiguous voluntary consent—would likely chill the research and development of innovative web-based products and services. In the end, consumers and the American economy would suffer most.

CONCLUSION

This Court should affirm.

Respectfully submitted,

/s/ Cory L. Andrews
Cory L. Andrews
John M. Masslon II
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Ave. NW
Washington, DC 20036
(202) 588-0302
candrews@wlf.org

February 15, 2024

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limits of Federal Rule of Appellate Procedure 29(a)(5) because it contains 3,758 words, excluding those parts exempted by Federal Rule of Appellate Procedure 32(f).

I also certify that this brief complies with the typeface and type-style requirements of Federal Rules of Appellate Procedure 32(a)(5) and (6) because it uses 14-point Century Schoolbook font.

/s/ Cory L. Andrews
CORY L. ANDREWS
Counsel for Amicus Curiae
Washington Legal Foundation

February 15, 2024