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 (GONZALEZ ROGERS, J)

BRIEF OF THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION AS *AMICUS CURIAE* SUPPORTING DEFENDANT-APPELLEE

STEPHANIE A. JOYCE
COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION
25 Massachusetts Avenue, NW,
Suite 300C
Washington, DC 20001
(202) 783-0070
stephaniejoyce@ccianet.org

Amicus Curiae

February 16, 2024

RULE 26.1 DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* states as follows:

The Computer & Communications Industry Association (CCIA) is a trade association operating as a 501(c)(6) non-profit, non-stock corporation organized under the laws of Virginia. CCIA has no parent corporation and no publicly held corporation owns 10% or more of its stock.

/s/ *Stephanie A. Joyce*
Stephanie A. Joyce

February 16, 2024

TABLE OF CONTENTS

STATEMENT OF *AMICUS CURIAE* 1

INTEREST OF *AMICUS CURIAE* 1

SUMMARY OF THE ARGUMENT 2

ARGUMENT 5

I. DIGITAL SERVICE PROVIDERS PLAY A PIVOTAL ROLE IN SUPPORTING AND IMPROVING THE DIGITAL ECONOMY 5

II. EXPANDING COMPANIES' LIABILITY RISK FOR PRIVACY POLICIES WOULD CREATE A STAGNANT INTERNET ECOSYSTEM. 9

CONCLUSION 13

CERTIFICATE OF COMPLIANCE 14

CERTIFICATE OF SERVICE 15

TABLE OF AUTHORITIES

Page(s)

Cases

F.B.T. Prods., LLC v. Aftermath Records, 621 F.3d 958 (9th Cir. 2010) 10

Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190 (N.D. Cal. 2014) 10-11

Smith v. Facebook, Inc., 745 F. App'x 8 (9th Cir. 2018) 10, 11

Other Authorities

Amazon, *Custom Advertising Solution*, Amazon Ads (2024) 5

CCIA, *The Sky Is Rising 2024 Edition*, CCIA Research Center (Jan. 2024) 6

CCIA, *Tools to Compete: Lower Costs, More Resources, and the Symbiosis of the Tech Ecosystem,* CCIA Research Center (Jan. 25, 2023).....8

Engine Advocacy, *Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups* (Mar. 2023) 11

Fed. Trade Comm'n, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (Mar. 2013) 10

Husch Blackwell, *State Privacy Chart: Applicability Threshold*, *Rights, Other Provisions* (Jan. 9, 2024) 12

Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, Fed. Trade Comm'n, Bureau of Econ. (Jan. 2020) 6

STATEMENT OF *AMICUS CURIAE*

This brief was authored entirely by the undersigned counsel and was funded entirely by the *amicus curiae*. No person or party other than *amicus curiae* contributed money to the creation, filing, or service of this brief. All parties have consented to the filing of this brief. Defendant-Appellee Google LLC is a CCIA member, but took no part in drafting this brief.

INTEREST OF *AMICUS CURIAE*

Amicus curiae Computer & Communications Industry Association (CCIA) is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For more than fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.

CCIA and its members have been leaders in the research, development, and implementation of countless digital services and products that have helped create the dynamic and open internet ecosystem of today. The legal issues in this case have the potential to impede the growth of the wider digital economy, raising significant concerns for CCIA and its members. Plaintiffs would like to establish an impossibly subjective standard for privacy policies adopted by online service providers,

exposing them to civil damages for failing to anticipate how any consumer might interpret their policy. This exponentially increased risk of liability would extend beyond browsers to encompass countless digital services that users, businesses, and the larger internet ecosystem rely upon every day. It would deter technology companies from improving their products and services (such as timely software patches) and prevent businesses of all sizes from using new innovative services (such as web hosting services) for additional security. CCIA files this brief to assist the Court in understanding the critical roles online service providers play in the digital economy and why a measured, balanced approach to privacy disclosures is necessary to preserve diversity, choice, and innovation in the online ecosystem.

SUMMARY OF THE ARGUMENT

The internet ecosystem continues to be an engine of economic growth and opportunity. Providers of website services have played a pivotal role in the development of this ecosystem by offering a wide array of digital tools and services, many of which users obtain at no or little cost. Website publishers have incorporated these new, affordable services to build upon the value and functionality of their sites, which in turn has allowed internet users to access previously unreachable markets. In this exchange, individuals consent to providing certain information, and that information makes their browsing experience richer, faster, and, in most cases, free of charge. This interaction between consumers, website publishers, and digital

service providers is the core of the internet. This dynamic ecosystem requires that organizations have flexibility to provide new features, along with security and privacy updates.

Organizations should be free to write general, clear policies that reasonably describe their collection and use of user-generated data. Responsible digital service providers have spent considerable time and resources to ensure that the privacy disclosures relevant to their products and services offer enough information and transparency that a consumer can meaningfully provide consent to the data collection and practices. The district court understood this dynamic and found that the disclosures Plaintiffs have challenged were sufficiently detailed such that a reasonable person would understand that Google receives data reflecting user activity on websites that use Google services and uses that data to customize services. The district court's grant of summary judgment for Google therefore should be affirmed.

CCIA supports affirmance of the district court's decision on two grounds. First, digital service providers play a pivotal role in maintaining and improving the digital economy. Specifically, providers of website services help power the innovation that benefits consumers, from real-time translation for travel and navigation to improved analytics productivity and features for e-commerce. Further, these services enable websites and applications to provide users with a broad range

of innovative features and functions. But in this lawsuit, Plaintiffs' positions risk disrupting and halting innovation within this mutually beneficial ecosystem.

Second, a commonsense approach to privacy policies and disclosures would help ensure that the digital economy continues to grow and improve. Small and medium-sized businesses presently are granted flexibility that allows them to continue innovating for the benefit of consumers, from security and privacy updates to new user controls and features. At the same time, users want more transparency into how their data is being collected and used by digital service providers to support and improve these innovative products and services. Responsible businesses strive to find a balance that is relevant to their users, providing sufficient details about their data practices without overwhelming users with overly technical language, thus enabling users to provide meaningful consent. Plaintiffs' aim, it appears, is to impose an overly prescriptive framework that would increase costs and create a worse online environment for all, in addition to conflicting with various state privacy laws that expressly regulate privacy notices and consent.

For all these reasons, the district court correctly granted Google's motion for summary judgment, and this Court should affirm.

ARGUMENT

I. DIGITAL SERVICE PROVIDERS PLAY A PIVOTAL ROLE IN SUPPORTING AND IMPROVING THE DIGITAL ECONOMY.

The dynamic digital economy represents a complex ecosystem where online service providers, advertisers, and consumers interact, shaping the way businesses operate and users engage with online products and services. Online service providers are the foundation of this ecosystem, supporting and improving these digital interactions. From analytics and payment processing to customer service and marketing tools, websites and applications have specialized in offering solutions that are tailored to specific needs within nearly every sector. Specifically, the rise of free to low-cost website services has provided businesses of all sizes access to the latest software, tools, and applications without having to purchase or maintain them, whose helpfulness increases as the services become more specialized. These web services and tools enable businesses to scale operations and improve the functionality of their website.

Website service providers have also enabled individuals and businesses to monetize their content through digital advertising. Improved efficiencies in advertising have benefited competition by allowing smaller businesses to utilize these ad services to connect with new markets and audiences.[1] In fact, the Federal

[1] *See Custom Advertising Solutions*, Amazon Ads,

Trade Commission Bureau of Economics noted in 2020 that the benefit of advertising takes various forms that include reduced search costs and greater price competition between firms.[2]

Importantly, consumers have benefited the most from this economic model: they enjoy an improved online environment. A tremendous amount of valuable online content is available to internet users at little or no cost.[3] In addition, the availability of ad-supported models has fostered this competition, which has benefited consumers in the form of improved options and features like seamless online shopping and personalized recommendations.

For many of these valuable web services and tools to work, however, various types of basic, non-personal information need to be transmitted between devices and across the network. Much of this information, such as IP addresses, helps devices find each other and communicate on the network. These data transmissions also

---

https://advertising.amazon.com/solutions/products/custom-solutions (last accessed Jan. 20, 2024) (explaining how pseudonymization can be used to protect users' privacy and still allow organizations to offer relevant and useful advertising).

[2] *See* Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, Fed. Trade Comm'n, Bureau of Econ. (Jan. 2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf.

[3] *See* CCIA, *The Sky Is Rising 2024 Edition*, CCIA Research Center (Jan. 2024), https://research.ccianet.org/reports/sky-is-rising-2024-edition/#main-content (explaining how the internet has enabled "more people to create, share, distribute, consume, and monetize creative works" than ever before).

allow for a website's implementation and use of third-party application programming interfaces (APIs), which help facilitate the exchange of data by allowing different software applications and systems to work together. APIs enable (1) service providers to integrate third-party functionalities into their websites, (2) advertisers to access and analyze relevant visitor data, and (3) consumers to enjoy a more interconnected digital experience. This transparent and efficient exchange of information via IP addresses and APIs lies at the center of the digital economy, empowering organizations to create and share digital resources. For instance, Google Maps' JavaScript API provides several types of data including landmark and location data. Businesses can integrate the information into their products and services, enabling improvements such as optimized food deliveries and improved ride-sharing services. APIs also rely upon other foundational functions like the Hypertext Transfer Protocol (HTTP), which provides a mechanism for APIs to transmit requests and responses over the internet.

HTTP represents one of the countless internet signals upon which users rely every day. Plaintiffs' positions in this litigation, however, would impose crushing liability risk for any firm that offers integrated web services, regardless of sector or use case, if an individual could cite any language from any disclosure, no matter how unrelated, belonging to the firm. Plaintiffs' proposed, greatly expanded, standard for consent thus would create massive liability exposure, disincentivizing companies

from offering integrated digital services including a wide range of security and performance features that contribute to a faster and more secure internet. Nor could companies explore offering additional services.

The consequence would be that businesses and other service providers would no longer benefit from improved security and performance including encryption that protects the data traveling between users' browsers and a web server. The entire internet ecosystem would deteriorate if technology companies were disincentivized from leveraging their expertise to offer new services, like mobile payment processing and cloud storage, unless they subjected themselves to multi-billion-dollar liability risk. This would adversely impact the availability and proliferation of free and low-cost web tools and services, which a 2023 CCIA report has found to help reduce barriers to entry and increase the flow of innovation into digital markets.[4] Plaintiffs' demands would restrict the sharing of routine and fundamental internet signals like IP addresses and HTTP to a degree that would disrupt the entire internet ecosystem, cause stagnation in the digital market, and limit consumer choice.

---

[4] *See* CCIA, *Tools To Compete: Lower Costs, More Resources, and the Symbiosis of the Tech Ecosystem*, CCIA Research Center (Jan. 25, 2023) (showing startups leverage dozens of technology services and tools like AWS, Slack, and Zoom to build and run their companies).

II. EXPANDING COMPANIES' LIABILITY RISK FOR PRIVACY POLICIES WOULD CREATE A STAGNANT INTERNET ECOSYSTEM.

Privacy policies and disclosures help promote a dynamic economy in which businesses are free to improve existing products and services for the benefit of consumers, and consumers can meaningfully provide informed consent to the sharing of their personal information that drives these advancements. Unfortunately, the privacy standard that Plaintiffs demand would impede companies' ability to protect consumer privacy. Requiring organizations to provide overly prescriptive policies and disclosures would result in a worse online environment for businesses and consumers. If Plaintiffs' arguments were to prevail, businesses would be prevented from improving their products and services, including their approach to providing users with important and relevant privacy and security updates, unless they had the resources to consistently and continuously overhaul their policies and disclosures.

Plaintiffs' proposed standard would also reintroduce, if not worsen, the risk of consume "consent fatigue," because a business would be forced to update their policies to inform users about each and every modification, including minor, routine changes to browser functionality or to a completely unrelated web service offered by the same company. Businesses also would be forced to specify every current, and *potential*, data use and practice with such specificity, including technical language,

that the disclosures would likely overwhelm users.

Here, the district court correctly held that Google did not exceed the scope of consent. Privacy policies and related disclosures require a balance between exhaustiveness and readability. *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8-9 (9th Cir. 2018) (finding broad general disclosure sufficient). Businesses should not be required to—and have never been required to—specify every detail and manner in which a business collects and uses the data, so long as they broadly disclose the collection and uses in a way ordinary users would understand. *See F.B.T. Prods., LLC v. Aftermath Records*, 621 F.3d 958, 964 (9th Cir. 2010) (holding that "[a] contractual term is not ambiguous just because it is broad.").

Businesses also must be free to draft disclosures in a way that is relevant and reasonable to their specific product or service. Thus, for example, the Federal Trade Commission has clarified in its *.com Disclosures* guidelines that so long as a disclosure is reasonable in the context of the method of data collection, then the disclosure is appropriate.[5] In addition, courts in this circuit have found it sufficient for companies to simply disclose enough information so that a reasonable user would understand that the company was collecting the data at issue. *See Perkins v. LinkedIn*

---

[5] *See .com Disclosures: How to Make Effective Disclosures in Digital Advertising*, Fed. Trade Comm'n (Mar. 2013), https://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.

Corp., 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014); *see also Smith*, 745 F. App'x at 9.

At the state level, businesses more and more are required to draft privacy policies that adhere to a growing list of requirements concerning the scope, readability, and even frequency of the notices and disclosures. Thirteen states now have comprehensive consumer privacy laws, with more expected this year. A 2023 report examining the costs encountered by startups found that even the smallest disparities between state privacy laws results in significant compliance costs, with an estimated cost of $10,000 per additional, new state statute "just to start reviewing and modifying policies for compliance."[6]

Despite this growing regulatory patchwork, state privacy laws, including in California, still largely recognize the importance of finding a balance between these important considerations. The regulatory approach to consumer privacy disclosures that is emerging at the state level offers a workable framework that empowers consumers with sufficient information while promoting innovation—it grants businesses necessary flexibility when drafting privacy disclosures and policies. In drafting these policies, companies generally do not need to specify every detail of

---

[6] *See* Engine Advocacy, *Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups* (Mar. 2023), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf.

their practices. While the specifics differ between states, each privacy disclosure must be transparent and clearly written in order that a user has enough information to provide meaningful consent.[7]

Companies must be free to write general, easy-to-understand policies that reasonably describe their collection and use of user-generated data. Companies should be encouraged to develop and offer multiple online services, with each contributing to a stronger internet ecosystem. Plaintiffs' positions impede efforts to improve and secure the digital services millions of people use every day. Customers benefit from the swift launch of new experiences and features, which they would be denied if a company had to restart the consent process for every new feature or update. Increasing the liability risk for disclosures—as Plaintiffs seek to do in this lawsuit—will slow down innovation and undermine the quality of digital services. In addition, such increased risk will deter organizations' research and investment in web products and services.

The claims in this lawsuit attempt to place upon Google the liability for the privacy practices and disclosures that every other online portal employs. Stated differently, Plaintiffs have sued Google simply because it happens to offer a web

---

[7] *See* Husch Blackwell, *State Privacy Chart: Applicability Threshold*, *Rights, Other Provisions* (Jan. 9, 2024), https://www.bytebacklaw.com/wp-content/uploads/sites/631/2024/01/New-Jersey-Chart.pdf.

browser as well as third-party website services. Not only would such a massive liability shift be unjust to Google, but it would discourage digital services companies from expanding their offerings for fear that disclosures for one service can be weaponized opportunistically against the functionality of another. Here, the district court appropriately considered whether Google itself had failed in its privacy practices and protections, and correctly found that it had not. Summary judgment therefore should be affirmed.

CONCLUSION

The district court's order granting summary judgment for Google should be affirmed.

February 16, 2024

Respectfully submitted,

/s/ *Stephanie A. Joyce*
Stephanie A. Joyce
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION
25 Massachusetts Avenue, NW
Suite 300C
Washington, DC 20001
Tel. 202.783.0070
stephaniejoyce@ccianet.org

CERTIFICATE OF COMPLIANCE

In compliance with Fed. R. App. P. 29(a)(4), I certify that, according to the word-count function of Microsoft Word, the foregoing brief Amicus Curiae contains 2,642 words, which is less than one-half the number of words that Fed. R. App. P. 32(a)(7) generally affords to a party for its principal brief.

/s/ *Stephanie A. Joyce*
Stephanie A. Joyce

CERTIFICATE OF SERVICE

I, Stephanie A. Joyce, hereby certify that on February 16, 2024, I electronically transmitted the foregoing document to the Clerk's Office using the CM/ECF System. I certify that all participants in this case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ *Stephanie A. Joyce*
Stephanie A. Joyce

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

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

I am the attorney or self-represented party.

This brief contains 2,642 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 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.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 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.
  - ☐ 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/Stephanie A. Joyce **Date** February 16, 2024
*(use "*s/[typed name]*" to sign electronically-filed documents)*