UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, *et al.,* Plaintiffs, v. GOOGLE, LLC, Defendant.	Case No. 1:20-cv-03010-APM HON. AMIT P. MEHTA
STATE OF COLORADO, *et al.*, Plaintiffs, v. GOOGLE, LLC, Defendant.	Case No. 1:20-cv-03715-APM HON. AMIT P. MEHTA

BRIEF OF THE FEDERAL TRADE COMMISSION AS AMICUS CURIAE IN SUPPORT OF PLAINTIFFS

Dated: May 9, 2025

CLARKE EDWARDS
Acting Director, Office of Policy Planning

KATHERINE WHITE
Deputy Director, Bureau of Consumer Protection

ANUPAMA SAWKAR
Acting Deputy Director, Office of Policy Planning

Attorneys for Amicus Curiae
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, DC 20580
Tel: 202-779-6023

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

INTEREST OF THE FEDERAL TRADE COMMISSION

The Federal Trade Commission ("FTC" or "Commission") is charged by Congress with protecting the public from deceptive or unfair business practices and from unfair methods of competition. The Commission also protects consumers from unlawful privacy and data security practices—through Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive trade practices, as well as a range of sector-specific statutes and regulations, including the Gramm-Leach-Bliley (GLB) Act's Privacy Rule, 16 C.F.R. Part 313, the GLB Safeguards Rule, 16 C.F.R. Part 314, the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506, the COPPA Rule, 16 C.F.R. Part 312, the Health Breach Notification Rule, 16 C.F.R Part 318, and the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x. As the nation's primary law enforcement agency for privacy laws, the Commission has brought more than two hundred cases to address privacy and data security-related concerns over the last three decades.

The Commission has a strong interest in ensuring that companies vigorously protect consumers' privacy. It also has long experience with crafting appropriate remedies for unlawful breaches of consumers' privacy. The Commission submits this brief to explain why the privacy protections in Plaintiffs' Revised Proposed Final Judgment are consistent with the Commission's own privacy and data-security orders. The Commission also notes the importance of these protections given Google's past alleged privacy violations. Finally, we explain why remedies that promote competition in monopolized markets can create healthy incentives for market participants (including the former monopolist) to compete on the quality of their privacy policies and technology—thereby improving privacy protections market-wide.

BACKGROUND

The Court found Google liable under Section 2 of the Sherman Act for maintaining monopolies in general search services and general search text ads. *United States v. Google LLC*, 747 F. Supp. 3d 1, 187-88 (D.D.C. 2024). Plaintiffs have now submitted a Revised Proposed Final Judgment ("RPFJ"). Pls.' Revised Proposed Final J., ECF No. 1184-1 (Mar. 7, 2025).

The RPFJ contains interrelated remedies designed to end Google's illegal monopolies over general search services and search text ads, restore competition that has been lost as a result of Google's unlawful conduct, and benefit consumers in the illegally monopolized markets. Most relevant to the privacy considerations addressed in this brief, the RPFJ requires Google to share targeted portions of its search index, user, and ads data with certain competitors for a limited period of time. RPFJ at 14. The RPFJ is designed to "make this data available in a way that provides suitable security and privacy safeguards." *Id.*

ARGUMENT

I. The RPFJ's Privacy Protections Are Consistent with Common Terms in the Commission's Privacy and Data Security Orders

The RPFJ would require Google to make available "User-side Data" to "Qualified Competitors." RPFJ at 16. "User-side Data" includes, among other things, "all data that can be obtained from users in the United States, directly through a search engine's interaction with the user's Device, including software running on that Device, by automated means." RPFJ at 7. Given the scope of this proposed data sharing, privacy considerations are critically important. The RPFJ accounts for these considerations by including terms that are consistent with those that the Commission includes in its own privacy and data security orders.

A. The RPFJ Contemplates an Independent, Expert Technical Committee to Help Ensure that Google and Qualified Competitors Protect Consumers' Privacy

Privacy programs that include independent auditing have been a keystone of the Commission's privacy and data security orders. While the specific requirements of such programs have evolved over time and depend on the nature and specifics of the alleged unlawful conduct, the Commission's orders generally share several features in common, including a requirement that the program must be documented in writing, and that the business (1) designate an employee to coordinate the program, (2) conduct risk assessments, (3) design and implement reasonable safeguards to control the identified risks, and (4) evaluate and adjust the program as necessary. *See, e.g.*, Decision and Order, *In re Global Tel*Link Corp.*, FTC Dkt. No. C-4801 (Feb. 23, 2024); Stipulated Order, *FTC v. Ring LLC*, Case No. 1:23-cv-1549 (D.D.C. June 16, 2023); Decision and Order, *In re Drizly, LLC*, FTC Dkt. No. C-4780 (Jan. 9, 2023); Decision and Order, *In re James V. Grago, Jr.*, FTC Dkt. No. C-4678 (June 19, 2019); Decision and Order, *In re GeneLink, Inc.*, FTC Dkt. No. C-4456 (May 8, 2014); Decision and Order, *In re Myspace LLC*, FTC Dkt. No. C-4369 (Aug. 30, 2012); Decision and Order, *In re BJ's Wholesale Club, Inc.*, FTC Dkt. No. C-4148 (Sept. 20, 2005).

The Commission has also typically required regular assessments of these programs conducted by a qualified, objective, independent third party. The third party must perform these assessments using generally accepted procedures and standards. *See, e.g.*, Stipulated Order, *United States v. Verkada, Inc.*, Case No. 3:24-cv-06153-CRB (N.D. Cal. Sep. 4, 2024); Stipulated Order, *United States. v. Epic Games, Inc.*, Case No. 5:22-cv-00518-BO (E.D.N.C. Feb. 7, 2023); Stipulated Order, *United States v. VTech Elecs. Ltd.*, Case No. 1:18-cv-114 (N.D. Ill. Jan. 23, 2018).

Finally, the Commission's privacy- and data security-related consent decrees and orders are subject to oversight either by the Commission itself or, when filed in federal court, by a federal judge. *See, e.g.*, Stipulated Order, *FTC v. Equifax Inc.*, Case No. 1:19-cv-03297 (N.D. Ga. July 23, 2019); Stipulated Order, *FTC v. D-Link Sys., Inc.*, Case No. 3:17-CV-00039-JD (N.D. Cal. Aug. 6, 2019); Stipulated Order, *FTC v. Vizio, Inc.*, Case No. 2:17-cv-00758 (D.N.J. Feb. 13, 2017). In either case, the ongoing ability of the Commission or the federal judge to monitor the defendant's compliance helps ensure that the defendant satisfies its obligations and that the remedy can be altered in the face of noncompliance or changed circumstances.

The RPFJ incorporates these common features in the Commission's data security and privacy orders. For example, the RPFJ ensures that independent third parties protect Google users' privacy through a "Technical Committee" (TC) appointed by the Court. RPFJ at 7. This TC would be composed of technical experts. *Id*. at 31 ("The TC members must be experts in some combination of software engineering, information retrieval, artificial intelligence, economics, and behavioral science."). It would also be fully independent from Google and competitors. *Id*. at 31 ("No TC member may have a conflict of interest that could prevent them from performing their duties in a fair and unbiased manner.").

Importantly, the TC would play a role on *both* sides of the User-side Data sharing contemplated by the RPFJ. With respect to Google, the TC would consult with Google to ensure that Google properly discharges its general duty to "safeguard[] personal privacy and security" before sharing any User-side Data, including through the use of "ordinary course techniques to remove any Personally Identifiable Information." RPFJ at 16-17. The TC would also consult with Google when considering the proper application of "anonymization or privacy-enhancing technique[s]" (discussed in more detail below). RPFJ at 17. Further, the RPFJ requires that

Google consult with the TC to "determine that . . . security and privacy safeguards [are] fully functional" before sharing any User-side Data. RPFJ at 17. With respect to recipients of Google's User-side Data, the TC would act as an independent auditor for any Qualified Competitor that might receive data from Google. Under the RPFJ, any Qualified Competitor must agree to "regular data security and privacy audits by the [TC]." RPFJ at 5.

B. The RPFJ Allows Google, in Consultation with the Technical Committee, to Use Anonymization and Other Privacy-Enhancing Techniques

The RPFJ allows Google to use "anonymization or privacy-enhancing technique[s]" to help protect consumers' privacy. RPFJ at 17. Permitting Google to use these tools, with oversight by the TC, provides an additional avenue for protecting users' privacy.

In its privacy and data security cases, the Commission has recognized that properly anonymized or "deidentified" data poses a reduced threat to privacy, and it has carved "deidentified" data out of certain order provisions. In recent orders regarding consumer privacy, the Commission has defined "deidentified" data so that companies understand the processes necessary to ensure that data is adequately deidentified—that is, it cannot reasonably identify, relate to, describe, be associated with, or be linked, directly or indirectly, to a particular person. *See, e.g.*, Decision and Order, *In re Mobilewalla, Inc.*, FTC Dkt. No. C-4811 (Jan. 13, 2025); Decision and Order, *In re Gravy Analytics, Inc.*, FTC Dkt. No. C-4810 (Jan. 13, 2025).

Privacy-enhancing techniques or technologies ("PETs") can provide another layer of protection for consumers. For more than a decade, the Commission has recognized PETs as part of a broader set of tools companies can use to protect user privacy. *See, e.g.*, Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 31, March 2012, *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-

protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (advocating for "ways to protect consumer privacy throughout the life cycle of . . . products and services, including through the development and deployment of PETs"). When properly implemented with safeguards to prevent the potential for the re-identification of data, PETs can help mitigate risks associated with data collection, storage, and sharing.

The RPFJ charges the TC with determining that appropriate safeguards, such as data anonymization and PETs, are "fully functional." RPFJ at 17. This is a clear directive: The TC should ensure that deidentification techniques and PETs are properly applied. This requirement reduces the risk of the misapplication of this technology and violations of consumers' privacy by both Google and any Qualified Competitor, consistent with other privacy and data security matters before the Commission. *See, e.g.*, Decision and Order, *In re Henry Schein Prac. Sols., Inc.*, FTC Dkt. No. C-4575 (May 20, 2016); Decision and Order, *In re Zoom Video Commc'ns, Inc*., FTC Dkt. No. C-4731 (Jan. 19, 2021); Decision and Order, *In re Residual Pumpkin Entity, LLC*, FTC Dkt. No. C-4768 (June 23, 2022).

II. The RPFJ's Privacy Protections Are Particularly Important Given Google's Past Lapses

Google's past lapses and failures to protect its users' privacy demonstrate both that independent TC oversight of Google's privacy obligations is important and that Google should not be uncritically presumed to have better privacy and data security practices than Qualified Competitors that would receive User-side Data—subject to TC oversight—under the RPFJ.

In 2011, the Commission brought an action against Google alleging that it engaged in unfair and deceptive practices in the rollout of its now-defunct social media network, Google Buzz. Decision and Order, *In re Google, Inc.,* FTC Dkt. No. C-4336 (Oct. 13, 2011). As alleged in the complaint, Google used information it obtained from its users when they signed up for

Gmail, repurposing that data without its users' consent to populate Google's social media service, Google Buzz. The Commission alleged that Google deceptively subverted user expectations by continuing to enroll users in Buzz features even if they had chosen to turn off the Buzz service. The company also represented that consumers would be able to control what kinds of information would become public through their Google profile, yet Google did not tell consumers that the identities of the people with whom they emailed and chatted the most would become public on Buzz by default.

In settling these allegations, Google agreed to implement a comprehensive privacy program; cease misrepresenting how it maintains and protects information about individuals; and subject itself to biennial privacy assessments conducted by an independent third party for 20 years. The order remains in effect until October 13, 2031. *See* Decision and Order, *In re Google, Inc.,* FTC Dkt. No. C-4336 (Oct. 13, 2011).

One year after the consent order was entered, the Commission alleged that Google violated the Commission's administrative order by misrepresenting to consumers using Apple's Safari browser that it would not place tracking cookies. Google agreed to settle the allegations and paid a $22.5 million civil penalty. *See United States v. Google, Inc.*, No. 3:12-cv-04177-SI, 2012 WL 5833994, at *2 (N.D. Cal. Nov. 16, 2012).

In September 2019, the Commission and the New York Attorney General entered into a settlement with Google and its subsidiary YouTube related to allegations that the video sharing service illegally collected personal information from children without their parents' consent. The FTC alleged that Google and YouTube collected, used, and/or disclosed personal information from children in violation of COPPA, 15 U.S.C. §§ 6501-6506, by failing to provide notice of the personal information they collected from children; failing to provide notice to parents of how

they used that information; and failing to obtain verifiable parental consent before any collection or use of personal information from children. *See* Stipulated Order, *FTC v. Google LLC*, Case No. 1:19-cv-02642 (D.D.C. Sept. 10. 2019). In the settlement with New York and the Commission, Google and YouTube agreed to pay $136 million to the FTC and $34 million to New York for violations of the COPPA Rule, 16 C.F.R. Part 312, and the companies agreed to take further steps to ensure they comply with COPPA.

III. The RPFJ's Requirement that Google Share Targeted Portions of Its Search Index Fosters Competition that Benefits Consumers

The benefits of competition extend beyond price and include "product variety, quality, [and] innovation." *United States v. Anthem, Inc.*, 855 F.3d 345, 370 (D.C. Cir. 2017). Conversely, the lack of competition in monopolized markets can inhibit the monopolist's incentives to compete on dimensions like product quality—including privacy-related measures of quality. *Cf. United States v. Microsoft Corp.*, 253 F.3d 34, 56 (D.C. Cir. 2001) (recognizing that Microsoft was able to stave off "even superior new rivals" because barriers to entry protected its monopoly "irrespective of quality").

Because of Google's monopoly power in general search services and general search text ads, Google has been insulated from the pressures to compete for users on the basis of its privacy policies and protections. *See Google*, 747 F. Supp. 3d at 55 (describing how Google considers "the business case for making privacy-focused changes"). This lack of competition has resulted in users having little choice but to accept whatever level of privacy Google chooses to provide. Remedies like the RPFJ that are designed to revive competition in general search services and general search text ads would create the incentive for Google and other market participants to compete on privacy and data protection, driving higher quality protection market-wide.

CONCLUSION

When an antitrust offense has occurred, the remedy should "effectively pry open to competition a market that has been closed by defendants' illegal restraints." *Int'l Salt Co. v. United States*, 332 U.S. 392, 401 (1947). A remedy like the RPFJ that seeks to restore lost competition through data-sharing requirements must account for privacy considerations and take steps to protect sensitive user data. The RPFJ does so in multiple ways that align with data-privacy elements that the Commission commonly includes in its own consent decrees and orders. Particularly in light of Google's past privacy lapses and the potential for a remedy in this case to spur newfound competition between search providers on their privacy tools and policies, Plaintiffs' RPFJ is well designed to protect user privacy as it seeks to "pry open" long-monopolized markets.

Dated: May 9, 2025

Respectfully submitted,

/s/ Anupama Sawkar

ANUPAMA SAWKAR
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, DC 20580
Tel: 202-779-6023
asawkar@ftc.gov

CLARKE EDWARDS
(D.C. Bar. No. 1011154)
Acting Director
Office of Policy Planning

KATHERINE WHITE
(D.C. Bar No. 90014584)
Deputy Director
Bureau of Consumer Protection

CERTIFICATE OF SERVICE

I hereby certify that on May 9, 2025, I electronically filed a true and correct copy of the foregoing Brief of the Federal Trade Commission as Amicus Curiae with the Clerk via the CM/ECF system which will send notification of such filing and service upon all counsel of record.

/s/ Anupama Sawkar

Anupama Sawkar
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
Tel: 202-779-6023