

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

United States of America, *et al.*,

Plaintiffs,

Case No. 1:20-cv-03010-APM

v.

HON. AMIT P. MEHTA

Google LLC,

Defendant.

State of Colorado, *et al.*,

Plaintiffs,

Case No. 1:20-cv-03715-APM

v.

HON. AMIT P. MEHTA

Google LLC,

Defendant.

JOINT STATUS REPORT

Pursuant to the Court’s Minute Order issued September 11, 2026, the Parties submit the following Joint Status Report updating the Court on the status of the Source Code Agreement.

I. Joint Status Update

The Final Judgment directs that the Technical Committee (“TC”) “shall have access to Google’s source code and algorithms, subject to a confidentiality agreement, as approved by the Plaintiffs and to be agreed to by the TC members pursuant to Section VII.A.8 below, and by any staff or consultants who may have access to the source code and algorithms.” Final J. § VII.A.7.d.

On April 14, 2026, Google provided Plaintiffs its first draft of the Source Code Agreement (“SCA”), which Plaintiffs shared with the TC. At that time, the first three members of the TC were

working to identify their selections for the remaining two positions on the TC, pursuant to Section VII.A.3.c. On May 9, 2026, the Court appointed the final two individuals. ECF No. 1517. As of June 15, 2026, all five members of the TC (“TC Members”) were fully onboarded.

On June 30, 2026, Plaintiffs sent Google a revised draft of the SCA. On July 14, 2026, the Parties held a meet and confer and discussed Plaintiffs’ proposal, including Section 3 of the agreement, which involves central issues such as determining what data and information is protected, who may access it, how it is accessed, what analytical tools will be provided, when the tools and data will be provided, and what security measures may be imposed, among other requirements. On July 31, 2026, Google sent Plaintiffs a revised draft, reserving comments on Section 3 pending further discussion. At Google’s request, on August 6, 2026, a call was held between an internal Google subject-matter expert and the TC to discuss issues related to Section 3. Plaintiffs followed up on those issues by letter to Google on August 7, 2026. The Parties exchanged further correspondence, and on August 13 and 14, 2026, two additional calls were held between the TC and subject-matter experts at Google—specifically, a managing director of security engineering and an engineering vice president at Google. On August 19, 2026, Plaintiffs sent Google a revised draft SCA.

On August 28, 2026, Google sent Plaintiffs a revised draft SCA, including comments on Section 3. The Parties met and conferred that same day. On September 4, Plaintiffs sent Google an updated draft, advising that Plaintiffs considered it to be the final version they intended to approve on September 9, 2026, and asking that Google confirm it would sign the agreement. The Parties met and conferred on September 8, 2026, during which Google stated that it continued to have questions regarding Section 3. On September 9, 2026, Plaintiffs sent Google the SCA as approved by Plaintiffs, attached hereto as Exhibit A. On September 10, 2026, Google sent Plaintiffs a letter

with questions regarding the SCA, including Section 3. On September 14, 2026, Google sent Plaintiffs a proposed SCA, attached hereto as Exhibit B. On September 16, 2026, the parties agreed to negotiate their proposals for the definition of “Authorized Persons” further, and the parties have agreed to exchange proposals on September 17, 2026.¹ Google has not signed Plaintiffs’ approved SCA, and Plaintiffs have rejected Google’s remaining substantive revisions to the SCA. The parties set forth position statements below.

II. Plaintiffs’ Position Statement

It is critical to the timely enforcement of the Final Judgment that Google promptly execute Plaintiffs’ approved SCA. *See* Ex. A. To continue making progress in implementing the remedies, the TC must be able to understand Google’s mechanisms for securing and operating critical system components. Being able to access and observe those systems in the first instance is a necessary predicate to that effort. The TC cannot currently do this because those systems fall within the scope of the SCA and Google has refused to provide access to those materials until after the SCA is in place.

Plaintiffs have worked to promptly conclude the SCA, conducting the necessary diligence while pushing to resolve issues quickly. Plaintiffs have long taken seriously the protection of Google’s source code and algorithms, proposing in their Initial Proposed Final Judgment in November 2024 that “[t]he TC will have access to Google’s source code and algorithms, subject to a confidentiality agreement, as approved by the Plaintiffs.” ECF No. 1062-1 at § X.A.7.e. Notably, Google actually *opposed* including a Source Code Agreement in the Final Judgment, but after the parties litigated this precise language, the Court ultimately used the language from Plaintiffs’

¹ The parties will update the Court at the Status Conference and may respectfully request the Court’s guidance if they are unable to reach agreement.

proposal in the Final Judgment. ECF No. 1462 (Final J.) § VII.A.7.d; *see also* ECF No. 1461 (Mem. Op.) at 75 (noting “[n]o similar provision” was proposed by Google with respect to Plaintiffs’ proposed Source Code Agreement provision).

Plaintiffs’ approved SCA satisfies the requirements of the Final Judgment and fully protects Google’s sensitive information. Indeed, the SCA empowers Google to decide which of its information is the most sensitive and to maintain such information on its own systems while also facilitating timely and necessary access for the TC members and staff implementing the Court’s Final Judgment. *See generally* Ex. A. By contrast, Google’s objections are attempts to relitigate resolved issues and, if implemented, would form a barrier to the effective enforcement of the Final Judgment. Plaintiffs therefore respectfully ask the Court to enforce the Final Judgment by instructing Google to enter into Plaintiffs’ approved SCA set forth in Exhibit A.

A. Plaintiffs’ Approved SCA Satisfies The Final Judgment By Providing Google Ample Protections Through Google’s Own Secure Environment

Plaintiffs’ approved SCA protects Google’s most sensitive source code, algorithms, and user-side data by maintaining this data within Google’s own computing environment, with limited, principled exceptions. Under Section 2.1 of the agreement, Google has the authority to designate—subject to challenge—materials and information that Google believes satisfy the criteria of “Google Highly Sensitive Information” (GHSI) set forth in Section 3.1. GHSI includes source code and algorithms, advertising auction data, user data, and associated documentation. The definition is purposefully broad to allow Google the flexibility to quickly and easily determine whether materials accessed by the TC are truly GHSI. Through this design, Google will receive the assurance that it can broadly designate materials that—with limited, necessary exceptions—stay within its own systems, while Plaintiffs and the TC will receive materials more quickly to facilitate the timely implementation of the Court-ordered remedies.

Under Section 3.2 of the approved SCA, users authorized by the TC² may access such materials through a secure virtual environment in a manner similar to how Google permits its employees to access such materials (“Inspection Environment”). To comply with legitimate and ordinary security processes, Google is allowed to monitor TC actions through this environment, as set forth in the processes in Section 3.7. It is through this Google-hosted environment that the TC will perform much of its work. As the TC must be able to perform certain analyses under the Final Judgment to carry out its functions—e.g., the highly technical analyses required for recommending privacy safeguards under Section IV.C.1—Section 3.3 of the approved SCA also describes the analytical capabilities of the Inspection Environment. These functionalities were recommended to Plaintiffs by the TC and are premised on providing the TC with the same functionality available to Google employees. This is consistent with the Court’s authorization of access to source code as well as with the TC’s powers under the Final Judgment. *See* Final J. §§ VII.A7.d (“The TC may study, interrogate, and interact with the source code and algorithms”), VII.A.7.c (granting the TC the ability, among other powers, to “obtain reasonable access to any system or equipment *which Google personnel have access*” and to “require Google personnel to provide documents, data, and other information . . . as the TC may reasonably direct” (emphasis added)).

To implement the Final Judgment, however, the TC must be able to remove its work product and other materials from the Inspection Environment. For example, Plaintiffs and the TC must prepare recommendations to the Court that will be supported by highly technical and sensitive data with respect to user-side data disclosures, syndication tapering rates, various licenses, ads

² Plaintiffs will not become Authorized Persons under the agreement and will not directly access Google’s GHSI through the Inspection Environment. Ex. A, § 3.2. Only the TC, its staff, and its consultants will access the Inspection Environment. Plaintiffs will access Google’s GHSI as provided to it by the TC, as set forth in § 4.5 and described *infra* at Part II.B.1.

auction reporting, and user-side data privacy and security. Thus, the approved SCA makes clear that the TC may share GHSI with both the Court and Plaintiffs. Ex. A, § 4. To facilitate this necessity, the agreement makes limited exceptions as to what material may be removed from this Google-hosted virtual environment and provides procedures for doing so. Section 3.5 makes clear that the TC’s derived work product may be removed from the virtual environment and placed on the TC’s systems. *Id.*, § 3.5. The TC may not make any verbatim reproduction of source code unless necessary to the TC’s analysis and reporting functions. *Id.* Any information removed from the Google-hosted virtual environment, of course, will still be maintained as “Highly Confidential” under the Protective Order,³ and the TC’s own computing environment is protected by a Security Plan that was designed by TC Members with years of security expertise, approved by Plaintiffs, and reviewed by and discussed extensively with Google.

In short, the approved SCA (1) provides Google the broad ability to easily designate information as subject to the agreement; (2) allows Google to secure data accessed by the TC in the exact way Google secures this data in its business; (3) provides the TC with sufficient access; and (4) limits the disclosure of information outside the secure environment to the legitimate and necessary enforcement of the Final Judgment by the TC, Plaintiffs, and the Court. The agreement therefore amply protects Google and satisfies Section VII.A.7.d of the Final Judgment.

B. Google’s Objections To Plaintiffs’ Approved SCA Run Afoul Of The Final Judgment, Seek To Relitigate Resolved Issues, And Threaten The Effective Enforcement Of The Final Judgment

Google’s various objections are improper, largely seeking to make additions that conflict with the Final Judgment, to relitigate issues that Google previously disputed (and lost on), and to

³ Ex. A at § 1 (Definition of “Google Highly Sensitive Information”); ECF No. 98 (Protective Order) ¶ 1.h.

erect barriers to effective enforcement with no benefit to the security of Google's information.

Plaintiffs address each of these in turn.

1. Google May Not Limit The Analytical Capabilities Required By The TC To Enforce The Final Judgment

Google objects to Section 3.3's list of analytical capabilities to be provided to the TC within the Inspection Environment. Google's objection is improper and should be rejected, as (1) Plaintiffs and the TC have clearly explained what analytical tools are necessary for the TC to carry out its assigned functions under the Final Judgment; (2) the Final Judgment is clear that the TC shall receive access to these tools; and (3) providing these required analytical tools to the TC through the Inspection Environment, rather than an external environment, benefits both the TC and Google.

First, and most importantly, the list of analytical capabilities listed in (a)-(e) in Section 3.3 of the approved SCA is the list of capabilities that the TC expects it will need after a careful analysis of how to perform its various duties under the Final Judgment:

(a) the internal tools, query engines, notebooks, pipelines, and test and simulation frameworks that Google personnel use to access, query, analyze, execute, test, and simulate the relevant systems and datasets; (b) standard analytical software, including Python and R, with commonly used statistical and machine-learning packages, SQL query tools, and code search and navigation tools; (c) the ability to execute code, run queries against the covered datasets, conduct simulations (including ad-auction simulations and ranking and retrieval experiments), analyze using AI tools such as Gemini AI, Claude Code, etc. as provided to senior Google engineers, and build, train, and run models within the environment; (d) computing and storage resources scaled to the analytical task, no less capable than those generally available to similarly situated Google engineering teams; and (e) other tools, software, ancillary data, and computational resources as are reasonably required to support the analytic work of the TC.

Ex. A, § 3.3.⁴ As Plaintiffs informed Google, this list was prepared with the TC’s assistance and is based upon the TC’s knowledge of standard analytical tools—including AI tools—used by technology companies, including Google’s engineers⁵ and Google’s Red Team.⁶

Further, this list has remained unchanged since Plaintiffs’ June 30 proposal. Ex. E, Ltr. from K. Herrmann to C. Yeager (Sept. 11, 2026). Not only have Plaintiffs discussed these capabilities and the SCA extensively with Google through meet and confers, letters, and emails, but Plaintiffs also offered Google direct conversations with the TC to address any technical concerns about the implementation of Section 3.3. Ex. F, Email from K. Herrmann to C. Yeager (July 17, 2026). Google waited *two weeks* before accepting this offer. The TC then met with a senior engineer at Google to discuss their requirements, answering questions from both Google’s counsel and its employees. Ex. G, Ltr. from K. Herrmann to C. Yeager (Aug. 7, 2026) (providing supplemental responses to questions from Google informed by TC analysis). The TC also met with an engineering vice president at Google on August 14, 2026, to walk through the technical aspects of Google’s engineering environment and its ability to accommodate the requests in Section 3, including explaining what specific analytical tools were necessary under Section 3.3. Ex. H, Ltr. from K. Herrmann to C. Yeager (Aug. 17, 2026). As confusion benefits no one, Plaintiffs have

⁴ Google opposes providing these specific tools and instead proposes punting the dispute of the exact tools the TC may receive to another day, proposing toothless language that the TC be provided “software, tools, and computing resources necessary to discharge . . . the Final Judgment.”). Ex. B, § 3.3.

⁵ Google still objects to the inclusion of these tools even though the company recently publicly confirmed that its engineers have access to Anthropic’s coding models such as Claude Code. *E.g.*, Ex. C, Business Insider, “Google finally lets all engineers use Anthropic’s Claude” (Sept. 14, 2026), available at <https://www.businessinsider.com/google-finally-lets-all-engineers-use-anthropics-claude-2026-9>.

⁶ *E.g.*, Ex. D, The Evolving Role of the Red Team in the Era of Agentic Security, Google Security (Aug. 13, 2026), available at <https://blog.google/security/the-evolving-role-of-the-red-team-in-the-era-of-agentic-security/> (explaining how Google leverages AI tools to test its security systems).

provided Google with every chance to understand the requirements of the SCA. Google nevertheless objects because it purportedly requires further information from the Plaintiffs and the TC. Yet, Google has had the exact list of analytical tools required by the TC for *over two-and-a-half months* with ample opportunity to ask as many questions as they like. This process must end at some point, however, as the implementation of the approved SCA cannot be delayed indefinitely while Google incrementally considers various ways to limit the TC's analytical tools. *See infra* Part II.C.

Second, Google's objection to Section 3.3 is improper because the Court has already resolved Google's objection and ordered that the TC shall receive access to the capabilities and accompanying data sought by the TC. Plaintiffs and Google extensively litigated every word of the Final Judgment, and the Court ordered that: the TC may use analytical tools on Google's source code and other sensitive information, Final J. § VII.A.7.d (the "TC may study, interrogate, and interact with the source code and algorithms in order to perform its functions and duties."); the TC may generally use Google's analytical tools, *id.* § VII.A.7.c.iii (the TC may obtain "reasonable access to any system or equipment to which Google personnel have access");⁷ and the TC may require Google to populate its data and information into those tools and systems, *id.* § VII.A.7.c.v (the TC may "require Google personnel to provide documents, data, and other information"). Thus, there can be no genuine question as to whether the TC may receive access to Google's analytical tools in the same manner Google's employees do: the Court has already ordered that the TC shall receive such access.

⁷ Consistent with this order, Google's revisions to Section 3.2, which seek to limit the TC's ability to access materials that Google's employees can, should also be rejected. Ex. B, § 3.2.

Third, having Google supply the TC with the required analytical tools in the Inspection Environment offers Google the most cost-efficient and secure way to provide the TC with the tools required to complete its job. It is important to provide context for Section 3.3. Although all of Google's information is already protected in this litigation by the Protective Order generally, the purpose of the SCA is to provide an additional layer of protection for Google's most sensitive data, given the level of access the TC will need. Allowing Google to host the Inspection Environment through which the TC will access this information not only allows Google (and not an external entity) to protect that environment, but it also significantly reduces Google's cost of complying with the Final Judgment, as it will not need to duplicate and transfer code, data, tools, models, etc., externally. But, to capture that benefit, the TC must be supplied with the analytical tools it needs within the Inspection Environment. That is, if Google does not supply these standard analytical tools in the Inspection Environment, then the TC will have to export the appropriate materials and data to an environment where the TC can use the necessary analytical tools to fulfill the terms of the Final Judgment. Such a scenario would increase the amount of information contained outside of an environment controlled by Google and would also increase costs to Google.⁸ Plaintiffs additionally seek to avoid that scenario so that the TC may efficiently plan how it will perform the analysis it must under the Final Judgment.

⁸ Counsel for Google has made vague reference to concerns that it may not be able to provide the standard analytical tools sought by the TC, but in the two-and-a-half months Google has had Plaintiffs' language in Section 3.3, Google has never provided (let alone substantiated) an objection stating that it cannot provide any specific tool. Given the TC's assurance that the tools requested are standard and considering the amount and quality of Google's engineering resources, Plaintiffs are confident that Google can implement Section 3.3. Nevertheless, Plaintiffs reserve the right to separately address any new objection, including through a supplemental position statement if necessary.

2. Google Must Not Be Allowed To Approve Or Reject What Information Can Leave The Inspection Environment

Google objects to Plaintiffs’ approved SCA as Google believes it must be given the right to approve what information may be removed from the Inspection Environment. Specifically, Google seeks, in its proposed Sections 3.5 through 3.5.5, to require the TC to ask Google for permission to remove TC Work Product and Google GHSI from the Inspection Environment. Google would fully control the “Clean Team” that evaluates TC requests, Ex. B., § 3.5.4, and the Clean Team has the power to reject any request if it “poses an unreasonable risk to the privacy of users, to Google’s security, or to Google’s intellectual property rights,” *id.*, § 3.5.5. Google may take up to five business days to make the decision, and it is never required to explain its actions to the TC. *Id.*, § 3.5.5. Google’s improper objection, and its flawed proposal, must be rejected.

Most importantly, Google’s proposal is unworkable. It provides Google with the power to unilaterally reject the removal of information from the Inspection Environment. It is not Google’s responsibility to decide what the TC needs, nor should it be. The TC is already limited under Plaintiffs’ approved SCA to removing materials that are “reasonably necessary to perform the TC’s duties.” Ex. A, § 3.5. Google purports to limit its rejection right only to material that “poses an unreasonable risk to the privacy of users, to Google’s security, or to Google’s intellectual property rights.” Ex. B, § 3.5.5. But, this Court has already rejected Google’s arguments that Google’s security, Google’s intellectual property, and user privacy are each an independent reason not to order any of the remedies. Google cannot now do an end run around the Court by imposing this approval process. Moreover, Plaintiffs are greatly concerned that Google will attempt to use its unilateral right to reject any effort by the TC to remove its Work Product and GHSI from the Inspection Environment based on these same objections.

Critically, Google also introduces significant delay through its proposed process. Each request by the TC will take five business days to get a response, and as noted above, Google is not required to explain to the TC why its request was rejected. *Id.*, § 3.5.5. If the TC wants to engage in Google’s proposed “appeal” process (which grants the TC the ability to appeal to Google after Google rejects their request), the TC must first spend time trying to discern the reason its request was rejected in the first instance. Then, once the TC submits their appeal, Google’s process sets *no deadline* for Google to respond. Ex. B, § 3.5.5. Thus, even for TC efforts to remove information from the Inspection Environment that are not ultimately argued before the Court—and there will be many—Google’s process will significantly slow the TC’s work. Such a process is a framework for further delay and should not be allowed.

Finally, Google should have no right to interfere with the free flow of communications between the TC and Plaintiffs in implementing the Final Judgment. As explained *supra* Part II.A, Plaintiffs will not be accessing the Inspection Environment. The TC, which has the expertise and understanding to make use of the systems and data in the Inspection Environment, will be doing so. Yet, the TC will need to communicate sensitive information to Plaintiffs in support of preparing recommendations to the Court, among other duties. If Google has any ability to control or delay the flow of such information, it could significantly harm Plaintiffs’ ability to implement the Final Judgment.

3. Google’s Insertion Of An Unnecessary Patent Prosecution Bar That Would Make TC Staffing Impossible Should Be Rejected

Google also seeks a patent prosecution bar for signatories (including Plaintiffs under Google’s proposal) to the SCA. Google’s proposal (1) imposes limitations that are facially absurd and would impose a tremendous burden on the ability of the TC to hire and retain staff; (2) finds no support in the Final Judgment; and (3) does little to protect Google’s intellectual property. As

shown below, Google seeks a lengthy bar to “being involved in the prosecution of patents or patent applications” for anyone who views Google’s GHSI in a dozen broad fields:

9. Patent Prosecution Bar. Absent Google’s written consent, Signatory shall not be involved in the prosecution of patents or patent applications relating to any of the following subject matters: query understanding, information retrieval, web search indexing, or crawling, ranking of web results or ad results, search or search ad syndication, digital ad auctions and pricing, machine learning, large language models, artificial intelligence (including but not limited to generative artificial intelligence functionality trained for, adapted for, or used in connection with web search), privacy-preserving search technologies, or web spam detection. This provision applies to the prosecution of patents or patent applications before any foreign or domestic agency, including the United States Patent and Trademark Office. For purposes of this paragraph, “prosecution” includes any activity related to (i) the preparation or prosecution (for any person or entity) of patent applications, including among others reexamination and reissue applications or (ii) directly or indirectly participating, drafting, amending, advising, or otherwise affecting the scope or maintenance of patent claims. To avoid any doubt, “prosecution” as used in this paragraph does not include representing a party challenging a patent before a domestic or foreign agency (including, but not limited to, a reissue protest, ex parte reexamination, inter partes reexamination, inter partes review, post grant review or covered business method review). This Prosecution Bar shall end two years after conclusion of Signatory’s role as a member of the TC or as a person assisting the TC.

Ex. B, § 9. Google does not try to limit its terms in any way, unflinchingly proposing patent bars in fields as broad as “information retrieval,” “large language models,” and “artificial intelligence” with no exceptions. *Id.* Google’s views on what constitutes “involvement” in a patent are even broader, banning someone even from “indirectly participating” or “advising” clients on the “scope or maintenance of patent claims” for two years. *Id.*

First, such broad limitations are of serious consequence to TC members, TC staff, and Plaintiffs who have answered the call to public service to remedy over a decade of Google’s unlawful conduct. This is no hypothetical: three of five TC members have patents to which Google’s patent bar applies. Under Google’s punitive language, for example, a signatory who currently owns patents may not be involved in seeking those same patents in foreign jurisdictions

or in maintaining those patents.⁹ Ex. B, § 9. Thus, Google is demanding that those members effectively give up significant portions of their patent rights so that Google can protect against an unlikely scenario (illegally absconding Google’s intellectual property) that is already prohibited by TC agreements and the law.

Google’s patent bar also carries significant post-TC employment restrictions that do an end run around and directly undermine the Court’s recent order—based on the Parties’ *agreed-upon* proposal—regarding the very same type of restrictions. During a status conference on July 14, 2026, the Court directed the Parties to try to resolve the TC Members’ request for greater clarity regarding the one-year restriction on post-TC employment set forth in Section VII.A.2.c. *See* ECF No. 1542 at 2–3. The Parties spent weeks negotiating a proposal, which the Court adopted in its order of August 25, 2026. ECF No. 1543, § II. Yet, Google’s patent bar would inject the very same type of ambiguity that the Court’s August 25 order resolves: For two years after ceasing work with the TC, former TC employees cannot be involved in work that could eventually be used in a patent application relating to patents comprehensively covering the areas of expertise for which they were hired to the TC in the first place. As just one example, this would effectively bar any TC employee from performing work for any company seeking to develop any intellectual property relating to any type of artificial intelligence. Moreover, Google’s patent bar would extend the scope of employers to which a post-TC employment restriction would apply beyond what is provided for in the Court’s August 25 order, as well as extend the duration of such a restriction *by an additional year*. Such a result is untenable.

⁹ Notably, Google provides no exception to its ban on “maintenance of patent claims” if Google is the entity potentially infringing upon a signatory’s patent rights, thus providing itself free access to signatories’ patents.

Moreover, in an unprecedented request,¹⁰ Plaintiffs are not spared under Google’s proposal. The federal and state attorneys, economists, and paralegals who may access Google’s GHSI while preparing recommendations pursuant to the Court’s Final Judgment would be restricted from advising or counseling clients regarding any matter where a patent from a dozen broad categories is involved. This is a significant restriction that would significantly limit these civil servants’ employment opportunities for a hypothetical risk where Google is already protected by this Court’s order and existing law.

Second, and critically, the Final Judgment grants TC access to “Google’s source code and algorithms, subject to a *confidentiality* agreement.” Final J. § VII.A.7.d. A. Even under the broadest imagination, work on patent prosecutions simply has nothing to do with confidentiality. As with other unrelated restrictions that Google seeks in this confidentiality agreement, Google had multiple years to propose these restrictions in proposed final judgments, to object to Plaintiffs’ proposed final judgments for not including these restrictions, or even to note this issue when the parties litigated the Final Judgment post-opinion. Google never did. Moreover, all TC members, staff, and consultants already are required to attest under the penalty of perjury—and subject to the jurisdiction of the U.S. District Court for the District of Columbia—that they will “not copy or use [Protected Information] except for the purposes of this matter.” Ex. I, Exhibit 3 to the Confidentiality Agreement. Protected Information encompasses all information covered by the SCA, and thus Google already has the assurance it seeks. Ex. A, § 1 (Definition of “Google Highly Sensitive Information”).

¹⁰ Plaintiffs found no example—for good reason—of a Court ordering a patent bar and other severe restrictions on the civil servants enforcing the antitrust laws for accessing materials already protected by a Protective Order.

Third, these heavy restrictions are unnecessary as Google is already protected by federal¹¹ and state¹² trade secrets laws and the patent process. Indeed, the patent process requires that an applicant be the original inventor, and anyone misappropriating Google's intellectual property cannot claim to be an original inventor. Notably, Google's own policies confirm these restrictions are not necessary. Google will not require a patent prosecution bar of its own employees, its in-house counsel, its outside counsel, or other external parties that view Google GHSI. Ex. J, Email from K. Herrman to C. Yeager (Sept. 16, 2026). Despite repeated requests from Plaintiffs, Google offers no explanation as to why Google believes Plaintiffs and the TC constitute a unique threat to misappropriate Google's intellectual property.

In sum, Google's trade secrets are already well-protected, and Google's restrictions on those performing a public service by implementing the Final Judgment against a repeat monopolist must be rejected.

4. Google's Insistence That Plaintiffs Unnecessarily Sign The Source Code Agreement Should Be Denied

Google demands that Plaintiffs be forced to sign a source code agreement in order to view materials Google designates as GHSI, and Google further proposes that Plaintiffs' access be limited in its proposed revisions to Section 4. This is not acceptable or necessary for several reasons.

First, Google's demand is entirely inconsistent with its position during the remedies phase. Having previously opposed requiring a source code agreement at all, Google cannot now be heard to complain that such an agreement will not be signed by Plaintiffs.

¹¹ For example, the U.S. Criminal Code prohibits the theft of trade secrets, see 18 U.S. Code § 1832.

¹² *See, e.g.*, Ariz. Rev. Stat. § 13-1820; Colo. Rev. Stat. § 18-4-408; 18 Pa. Cons. Stat. § 3930; Utah Code § 76-6-401 *et seq.*

Second, Google’s demand would insert into the Final Judgment a new substantive requirement that Google never once previously raised. As noted in Part II *supra*, it was Plaintiffs that proposed the Final Judgment provision requiring a source code agreement for the TC, and Plaintiffs purposefully only included TC members and staff so that Plaintiffs’ ability to enforce the Final Judgment and abide by their ethical obligations were not impacted in any way. At no point did Google assert that if such an agreement were to be required, then Plaintiffs must also sign it. The Final Judgment reflects Plaintiffs’ approach, requiring only that the SCA be “agreed to by the TC members . . . and by any staff or consultants who may have access to the source code and algorithms.” Final J. § VII.A.7.d.

Third, the parties *already* negotiated and resolved whether Plaintiffs may view source code and other sensitive materials in the Protective Order. ECF No. 84, § 1(h). Section 11(b) of the Protective Order authorizes Plaintiffs to access “Highly Confidential Information” which specifically includes “trade secrets, including algorithms and source code; . . . [and] sensitive personally identifiable information.” *Id.*, § 11(b). Under the Protective Order, Plaintiffs have been entrusted with such sensitive materials for *over six years* in this case—*see, e.g.*, UPXD104 at 44,¹³ depicting productions of 7 days of query data by Google and Microsoft—and there is no basis for Google to now demand that Plaintiffs be subject to new and additional restrictions.

C. Google’s Delays Threaten The Timely Enforcement Of The Final Judgment

In addition to the above disputes, Plaintiffs must specifically address Google’s argument that more time is necessary to resolve lingering disputes with respect to Section 3. The Court

¹³ Prof. Michael Whinston Presentation: Monopoly Maintenance & Competitive Harm (Oct. 16-17, 2023), redacted version available at <https://www.justice.gov/atr/us-and-plaintiff-states-v-google-llc-2020-trial-exhibits>.

should disregard that assertion, as any more time provided to Google will come at the cost of further delaying the TC’s work on the Final Judgment.

Google has taken the position since at least as early as July 27 that it will not provide to the TC certain information that will be subject to an SCA until that SCA is resolved. *See, e.g.*, Ex. K, Email from K. Herrmann to C. Yeager (July 28, 2026); Ex. L, Ltr. from C. Connor to the TC (Aug. 14, 2026) (explaining that Google will not produce a requested protocol buffer schema “which describes the data used for Glue, among other uses”). Yet, Google has unnecessarily delayed the negotiation of the SCA, and in particular Section 3.

As discussed in greater detail *supra* Part II.B.1-2, Section 3 of the SCA is the most important section of the agreement, describing the Inspection Environment and the timing for provision of data and tools.¹⁴ On June 30, merely two weeks after onboarding the final two TC members (who have been serving as the lead technical liaisons with respect to the TC), Plaintiffs sent a proposed Section 3 to Google. Despite Plaintiffs’ repeated requests, however, Google did not provide a written response to that Section until August 28, i.e., *two months after* receiving Plaintiffs’ proposal.

Plaintiffs will not rehash the entire, extensive negotiation history for the Court, although the timeline set forth in Part I (Joint Status Update) above reflects Google’s lethargic approach to resolving the SCA. Those delays directly impact the work of the TC, because the TC needs information that Google withholds to perform its role under the Final Judgment. Google’s pattern of delay and impact on the TC weigh heavily in considering how Google may use any additional

¹⁴ Here again, Google seeks to inject process delays, rejecting Plaintiffs’ proposed language that Google have 10 business days to supply the Inspection Environment with datasets and tools specifically requested by the TC. Google instead proposes *no deadline* for it to ever provide materials it is under Court order to produce, only that it must notify Plaintiffs if it will take longer than ten business days. Ex. B, § 3.1. This, too, should be rejected.

time provided by the Court. Plaintiffs therefore respectfully request that the Court reject any effort by Google to delay the finalization of the SCA by seeking additional time to negotiate.

III. Google's Position Statement

Google remains committed to working constructively with the Technical Committee to provide robust, secure, reasonable, and flexible remote access to Google's source code, algorithms, and relevant datasets as required under the Final Judgment. To that end, Google is building a custom Chromebook-based Inspection Environment capable of executing analytical workflows, running data queries, and scaling compute resources to support the Technical Committee's oversight functions. Plaintiffs' demand, however, for *unqualified* access to Google's internal data, code, and systems is technically impracticable, incompatible with Google's infrastructure and policies, and unsupported by the Final Judgment. Google respectfully requests that the Court adopt its proposed request-based access framework and additional protective provisions, which meet the requirements of reasonable access in the Final Judgment and balance the Technical Committee's oversight needs with security and operational realities.

The Parties' Dispute Regarding Access. The parties' Source Code Agreement negotiations have concerned the technical capabilities of the "Inspection Environment," through which Google will provide the Technical Committee with "reasonable" remote access to Google source code, algorithms, and user data as required to "monitor Google's implementation of and compliance with its obligations under the Final Judgment." ECF No. 1462 § VII.A.7.a, d. Google has worked to accommodate the Technical Committee's requests, including developing a first-of-its-kind and flexible solution designed to meet the Technical Committee's stated needs for a remote environment and the Final Judgment's directive that the Technical Committee "may study,

interrogate, and interact with [Google’s] source code and algorithms in order to perform its functions and duties[.]” ECF No. 1462 § VII.A.7.d.

The dispute with Plaintiffs primarily involves their request that Google provide the Technical Committee *unqualified* access to unspecified “pipelines, and test and simulation frameworks that Google personnel use to access, query, analyze, execute, test, and simulate the relevant systems and datasets” and “the ability to . . . conduct simulations . . . and build, train, and run models within the environment.” Ex. A § 3.3. Plaintiffs appear to be demanding unfettered access to run unspecified tests and models over unspecified Google data within unspecified Google systems, with language that is not qualified by any standard of “reasonableness,” any nexus to the Technical Committee’s functions under the Final Judgment, or any opportunity for Google to object to access requests.

Google cannot accommodate these capabilities because its systems are designed to prohibit such undefined access; Google’s own engineers and executives lack the necessary permissions to do what the Plaintiffs have posed. *See* Ex. M (Declaration of Heather Adkins, Google’s Vice President of Security Engineering) ¶¶ 8–9, 20–26; Ex. N (Declaration of Isabelle Stanton, a Senior Director of Engineering at Google) ¶¶ 8–21. For Google’s security and infrastructure teams to design the “how” of access, Google needs a clearer understanding of the “what.” Ex. M ¶ 23. The Technical Committee would need to specify (for example) the test they seek to conduct. Google’s objection is thus not a function of Google seeking to delay, deny, or unreasonably limit the Technical Committee’s access to data and systems that are available in the ordinary course of business to Google employees, but rather reflects the reality of how Google’s systems are designed. The impracticality of Plaintiffs’ proposal is aggravated by a requirement that would obligate

Google to make any requested functionality available within two business days, an impossible timetable given the complexities of the systems and data at issue.

In addition to being impracticable, Plaintiffs' request finds no support in the Final Judgment. The Final Judgment provides that the Technical Committee may "monitor Google's implementation of and compliance with its obligations under this Final Judgment" and that one of the means by which the Technical Committee may do so is through "obtain[ing] *reasonable* access to any system or equipment to which Google personnel have access" "on *reasonable* notice to Google." ECF No. 1462 § VII.A.7 (emphasis added). The Inspection Environment capabilities to which Google has committed lay the foundation by which Google will provide this access, and Google will field the Technical Committee's particularized requests for access to specified systems and equipment as they are posed. For example, Google understands from the Technical Committee that they will need access to perform privacy "red teaming" (an exercise designed to test the adequacy of contemplated privacy-enhancing techniques), and Google is preparing those capabilities. But requiring Google to provide the *unbounded* access contemplated by Plaintiffs' language would not only exceed the scope of the Final Judgment, but would also run afoul of the Fourth Amendment's prohibition on unreasonable searches and seizures.

The Parties' Disputes Regarding the Removal and Use of Material from the Inspection Environment. In addition to the dispute over the scope and capabilities of the Inspection Environment, the parties have several additional disputes regarding provisions of the Source Code Agreement that Google considers critical to protect its intellectual property and user data from unauthorized use and disclosure. In particular, Google proposes: (1) a process by which the Technical Committee seeks Google's consent before removing material, including highly sensitive intellectual property, from the Inspection Environment; (2) that Plaintiffs' representatives who seek

access to Google’s source code and user data agree to the protections afforded by the Source Code Agreement; and (3) that individuals who obtain access to Google’s data agree not to file for a patent in related fields during the course of their work and for two years thereafter.

I. Factual and Procedural Background

A. Google Is Building a Remote Environment By Which the Technical Committee Can Access Google’s Source Code, Algorithms, User Data, and other Highly Sensitive Data.

Section 7 of the Final Judgment instructs that the “[t]he TC shall have the power and authority to monitor Google’s implementation of and compliance with its obligations under this Final Judgment,” and further provides:

- c. The TC may, on reasonable notice to Google:
 - i. interview, either informally or on the record, any Google personnel . . .;
 - ii. inspect and copy any document in the possession, custody, or control of Google personnel;
 - iii. obtain reasonable access to any system or equipment to which Google personnel have access;
 - iv. obtain reasonable access to, and inspect, any physical facility, building, or other premises to which Google personnel have access; and
 - v. require Google personnel to provide documents, data, and other information, and to submit reports to the TC containing such material, in such form as the TC may reasonably direct.

- d. The TC shall have access to Google’s source code and algorithms, subject to a confidentiality agreement, as approved by the Plaintiffs and to be agreed to by the TC members pursuant to Section VII.A.8 below, and by any staff or consultants who may have access to the source code and algorithms. The TC may study, interrogate, and interact with the source code and algorithms in order to perform its functions and duties, including the handling of complaints and other inquiries from third parties.

ECF No. 1462 § VII.A.7.

All parties recognize that access to Google Highly Sensitive Information (HSI) requires special safeguards, which the Source Code Agreement serves to provide. The parties also agree that the following types of material may be appropriately designated as Google HSI:

- (a) source code and Algorithms relating to any product, system, or conduct covered by the Final Judgment;
- (b) advertising auction data, including Search Text Ad (as defined in the Final Judgment) auction mechanics and design documentation, bidding, pricing, and reserve data, auction logs, and related configuration and experiment data;
- (c) user data, including User-side Data (as defined in the Final Judgment) and the data used to build, train, or operate the GLUE and RankEmbed model(s);
- (d) associated documentation, configuration files, build and test environments, and internal analyses.

Ex. A § 3.1; Ex. B § 3.1.

All parties further recognize that Google HSI will be accessed through a remote “Inspection Environment,” rather than through transmission of documents and data to the Technical Committee via file share for uploading directly to their systems. Hosting the data in a secure Inspection Environment provides an additional layer of security that is not possible where data is removed or “exfiltrated” from a Google-hosted environment into another environment. Ex. M ¶ 7.

At the Technical Committee’s request, Google is building this remote Inspection Environment for the Technical Committee and its staff on Google-managed Chromebooks. Ex. M ¶¶ 11–19. The Chromebooks will provide the Technical Committee and staff with their own enterprise workspace (a collection of Google cloud-based productivity, communication, collaboration, and storage tools) and an isolated development and testing environment (the Google Cloud Instance). *Id.* ¶ 15. Google will make requested source code, algorithms, and User-side Data available in the Google Cloud Instance, where the Technical Committee and its staff can “study, interrogate, and interact with the Google source code,” data, and algorithms without impacting other Google systems or code. ECF No. 1462 § VII.A.7.d; *see* Ex. M ¶ 16; Ex. N ¶ 7.

Google is also configuring the Chromebooks with the capability for the Technical Committee to potentially obtain appropriate limited access to systems on Google’s intranet (i.e., the virtual

environment in which Google employees actually interact with data and code on a day-to-day basis). Ex. M ¶ 18. Google stands ready to grant this limited access to the Technical Committee in response to specific reasonable requests if the access or capabilities sought by the Technical Committee exceed what the Google Cloud Instance can accommodate. *Id.* (To date, the Technical Committee’s requests have not required this access; the information requested can readily be provided through the Google Cloud Instance.) To ensure that the Technical Committee and its staff receive dedicated support, Google has designated personnel responsible for coordinating and facilitating the access necessary for the Technical Committee to fulfill its responsibilities under the Final Judgment. Ex. M ¶ 19.

A significantly more complicated aspect of the Plaintiffs’ request is that the Chromebooks provide capabilities by which the Technical Committee can “build, execute, and test the relevant systems in a non-production setting” and “access [] the internal simulation and evaluation frameworks (including for ad-auction, ranking, and retrieval experiments) that Google uses internally.” Ltr. from K. Herrmann to C. Yeager at 2 (Aug. 7, 2026). Plaintiffs have described this as a request for an “environment that reflects the working environment of a senior Google engineer, appropriately scoped and instrumented for oversight.” *Id.* Google has been working diligently to understand and operationalize this request, including by standing up an internal working group to design and implement the system. Dozens of Google personnel have contributed to the undertaking, including: Cloud Security, Access Security, Enterprise Security Operations, Endpoint Security, and Detection and Response employees from Google’s Security Engineering teams; employees from Google’s Technical Risk Management and Corporate Engineering teams; Extended Workforce Solutions employees from Google’s Global Business Organization; Vendor Management Operations employees from Google’s Global Affairs department; and product managers, engineers, and executives from Google’s Search and Ads teams. Ex. M ¶¶ 13–14.

A threshold practical challenge of the Technical Committee's request is that whereas Google employee access to systems is scoped to the employee's specific role and responsibilities (i.e., the tasks they need to perform to do their job), the Technical Committee's request is not tethered either to specific systems or to specific engineering tasks. *See* Ex. M ¶¶ 7–9, 22–23, 25–26; Ex. N ¶¶ 10–19. An additional practical challenge is that Google's systems are bespoke, and knowledge of and the ability to work with any particular system is highly decentralized across infrastructure and human resources. Ex. M ¶ 24; Ex. N ¶¶ 20–21. In the Technical Committee's interview with Google VP Liz Borowsky, the Technical Committee explained that a driving reason for their broad framing is that they do not yet know precisely which systems and capabilities they need. Google appreciates and understands that the Technical Committee is not in the position today to provide those specifics, as they are still in the process of orienting to Google's systems and working through the information Google has provided in its responses to the Technical Committee's initial round of information requests. As the Technical Committee provides additional specifics regarding what tasks they seek to perform (e.g., what observations or analyses they want to conduct) and which members and staff require the access, Google can scope and provision the access accordingly.

With this background in mind, Google has committed (in its proposed Section 3.3) to make available via the Inspection Environment:

- (a) standard analytical software, including Python and R, with commonly used statistical and machine-learning packages, SQL query tools, and code search and navigation tools;
- (b) the ability to execute code and run queries against relevant datasets;
- (c) computing and storage resources scaled to the analytical task and necessary to discharge all applicable responsibilities under the Final Judgment; and
- (d) other Google-provided tools, software, ancillary data, and computational resources as are reasonably necessary to support the analytic work of the TC.

Ex. B § 3.3. What Google has been unable to operationalize is the Plaintiffs’ request that the Inspection Environment additionally provide “full access to the software, tools, and computing resources necessary to run data analytics and simulations,” including specifically:

“the internal tools, query engines, notebooks, pipelines, and test and simulation frameworks that Google personnel use to access, query, analyze, execute, test, and simulate the relevant systems and datasets” and

“the ability to . . . conduct simulations (including ad-auction simulations and ranking and retrieval experiments), analyze using AI tools such as Gemini AI, Claude Code, etc. as provided to senior Google engineers, and build, train, and run models within the environment.”

Ex. A § 3.3. The capabilities Plaintiffs request—for example, pipeline access; test and simulation frameworks; and the ability to build, train, and run models—are highly dependent on the particular system and task. Ex. M ¶ 23. While Google can commit to provide the tools, software, data, and computational resources that the Technical Committee reasonably requires, Google cannot commit to the request as written abstracted from specifics. Enabling the necessary access, permissions, and compute power requires identification of the relevant systems and data. Ex. M ¶ 23; Ex. N ¶¶ 10, 18–19. And Google likewise cannot responsibly commit to providing access within two business days of a request, regardless of the nature of the request and without exception.

B. Google’s Proposal Includes Additional Protections Governing the Removal and Use of Its Source Code, Algorithms, User Data, and other Highly Sensitive Data.

In the course of the negotiation over the Source Code Agreement, Google and Plaintiffs discussed a range of issues beyond the specifics of the Inspection Environment. Although Google and the Plaintiffs successfully reached resolution on most provisions, three additional points of impasse remain.

First, Google proposes certain protections relating to requests from the Technical Committee or its staff to remove Google HSI from the protected Inspection Environment. Google appreciates that the Technical Committee may need to remove certain Google HSI from the Inspection Environment, for instance, to facilitate submissions to the Court. At the same time, permitting the unfettered removal of Google’s user data and source code presents clear risks to users’ privacy, system security, and Google’s intellectual property rights. Ex. M ¶¶ 7, 27–29. To balance those competing considerations, Google proposed that removal requests would be reviewed by a “clean team” of personnel at Google who are not involved in the underlying litigation, and who can ensure that the removal does not pose an unacceptable privacy, security, or intellectual property risk. Ex. B §§ 3.5.2, 3.5.3, 3.5.4, 3.5.5.

Second, Google seeks to extend the protections afforded by the Source Code Agreement to that Google HSI provided by the Technical Committee to Plaintiffs. *See, e.g.*, Ex. B § 4.5; *see also id.* (preamble & signature block). Google asked Plaintiffs to designate the personnel who would receive access to Google HSI and to have them execute a copy of the agreement. Plaintiffs refused, taking the position that anyone affiliated with the Plaintiffs may receive access to Google HSI that the Technical Committee removes from the Inspection Environment without any protections beyond what is in the operative Protective Order. While Plaintiffs indicated that they are ethically or legally prohibited from signing onto the Source Code Agreement, they have refused to identify which provisions are problematic or what the specific concern is so that Google can attempt to resolve the concern (whether by exempting them from the offending provisions or entering a supplemental protective order in lieu of their signing the Source Code Agreement).

Third, Google proposes to incorporate a patent-prosecution bar into the agreement. Ex. B § 9. A patent-prosecution bar is a routine feature of protective orders in litigation involving source

code and other intellectual property. It prohibits a person who sees highly sensitive information (like source code) from applying for a patent in the same space as the confidential material they saw. In that respect, it ensures that a party exposed to confidential technical material in litigation cannot use that technical information (even subconsciously) to craft an application for a patent.

C. Procedural Status of the Source Code Negotiations

Google provided an initial draft of the Source Code Agreement on April 14, 2026, containing comprehensive access provisions in Section 3. Following the onboarding of the fifth and final Technical Committee member, Plaintiffs responded with their counterproposal to Section 3 on June 30. To attempt to resolve operational concerns raised by Plaintiffs' sweeping access proposal, Google consulted technical leads familiar with the Researcher Integrated Data Groundwork Environment (RIDGE)—a virtual machine model that Google has used for similar circumstances, including for providing access to outside experts and regulators under Article 6(11) of the EU Digital Markets Act. After consulting with Google Technical Program Manager Yi Liao on August 6, however, the Technical Committee indicated that RIDGE would not suit its needs. Beginning in a subsequent technical discussion on August 13, Technical Committee members suggested adapting Google's standard vendor-onboarding workflow using provisioned Chromebooks. Google evaluated this approach and confirmed that while Chromebook-based access is feasible for certain tasks, the request for unqualified access and capabilities equivalent to that of a senior Google engineer presents a number of complex challenges. To bridge these differences, Google revised Section 3 to incorporate the Technical Committee's feedback, establish a request-based access model, and remove commitments that Google has concluded are infeasible or impossible (or otherwise incompatible with Google's systems) as posed. In response, Plaintiffs largely maintained their original language. Google has posed a number of technical questions—

designed to try to understand the specific capabilities that the Technical Committee seeks so that Google may design a solution—but Plaintiffs have declined further conferrals. *See, e.g.*, Ex. O.

II. Argument

A. The Technical Committee Should Make Particularized, Rolling Requests for Information and Access.

With respect to the access provisions of the Source Code Agreement, Google respectfully requests that the Court direct the parties to enter into an agreement that contains the following basic features. *First*, the Technical Committee should not be afforded *carte blanche* access to Google’s systems; rather, the Technical Committee should make requests for the information and access necessary to discharge its responsibilities under the Final Judgment. And *second*, Google should be presumptively afforded ten business days to field requests, subject to the Technical Committee’s ability to ask for an expedited response and Google’s ability to request additional time for particularly complex requests.

1. Scope of Access

To begin, the best way to ensure that the Technical Committee has the information that it needs is for it to issue particularized requests to Google for access and information necessary to discharge its responsibilities under the Final Judgment. Although Plaintiffs’ latest version of the Source Code Agreement contemplates that the Technical Committee will make rolling requests, *see* Ex. A § 3.1, other language in the agreement presupposes that the Technical Committee will have broad access to Google’s network “in the same manner as provided to Google employees,” *see id.* § 3.2, provisioned with analytical capabilities that are impracticable if not impossible to accommodate. The language implicated in this dispute is as follows: plain black text shows the agreed language; strike-throughs show the language that Google has requested to remove; and red text reflects Google’s proposed additions:

3.1 Covered Material; Prompt Availability. GHSI includes: (a) source code and Algorithms relating to any product, system, or conduct covered by the Final Judgment; (b) advertising auction data, including Search Text Ad (as defined in the Final Judgment) auction mechanics and design documentation, bidding, pricing, and reserve data, auction logs, and related configuration and experiment data; (c) user data, including User-side Data (as defined in the Final Judgment) and the data used to build, train, or operate the GLUE and RankEmbed model(s); (d) associated documentation, configuration files, build and test environments, and internal analyses. Google shall make reasonable best efforts to accommodate requests for material necessary to discharge Signatory's responsibilities under the Final Judgment. Material in categories (a)–(d) requested prior to the Effective Date shall be available to Authorized Persons under this Agreement within ten (10) business days of the Effective Date. Access to material in categories (a)–(d) requested more than ten (10) business days after the Effective Date shall **presumptively** be available to Authorized Persons under this Agreement within ~~two~~ **ten (2 10)** business days from the date of the request, **or such shorter period as the TC reasonably directs where its duties so require. Where Google believes it will take longer than these timelines, Google will provide notice within five (5) business days.**

3.2 Primary Form of Access: Google Corporate Engineering Environment. Google shall make GHSI available through **Google-managed** Chromebook computers that are issued to Authorized Persons, ~~enrolled in Google's corporate device management, and provided secure limited access to Google corporate network~~ in **the manner necessary to permit Signatory to discharge his or her responsibilities under the Final Judgment** ~~the same manner as provided to Google employees and contractors~~ (the "Inspection Environment"). The Inspection Environment shall be accessible to Authorized Persons on a continuous basis (24 hours per day, 7 days per week, subject to reasonable scheduled maintenance).

3.3 Analytical Capability. Subject to the provisions of Section 3.7, the Inspection Environment shall provide Authorized Persons with full access to the software, tools, and computing resources necessary to **discharge such Authorized Person's responsibilities under the Final Judgment** ~~run data analytics and simulations~~, including at a minimum: (a) ~~the internal tools, query engines, notebooks, pipelines, and test and simulation frameworks that Google personnel use to access, query, analyze, execute, test, and simulate the relevant systems and datasets;~~ (b) ~~standard analytical software, including Python and R, with commonly used statistical and machine-learning packages, SQL query tools, and code search and navigation tools;~~ (c) ~~the ability to execute code;~~ **and** run queries against **relevant** ~~the covered datasets;~~ ~~conduct simulations (including ad auction simulations and ranking and retrieval experiments);~~ analyze using AI tools such as Gemini AI, Claude Code, etc. as provided to senior Google engineers, and build, train, and run models within the environment; (d) ~~computing and storage resources scaled to the analytical task~~ **and necessary to discharge all applicable responsibilities under the Final Judgment,** ~~no less capable than those generally available to similarly situated Google engineering teams;~~ and (e) ~~other Google-provided tools, software, ancillary data, and computational resources as are reasonably required~~ **necessary** to support the analytic work of the TC. ~~Configurations that render the environment review only, or that prevent execution, querying, or simulation, are inconsistent with Section VII.A.7.d of the Final Judgment and shall not be imposed.~~

Plaintiffs’ proposal is both impracticable and unlawful. To be sure, Google understands why broad access to Google’s systems and datasets may look superficially appealing: The Technical Committee cannot foresee all the requests it may issue over the next half-decade. While it is understandable that the Technical Committee might therefore wish to request broad access and sort out the details later, that is, in practice, no solution.

As described in the Declarations of Heather Adkins and Isabelle Stanton, no single Google employee is likely to have access to the tools, systems, and knowledge necessary (for instance) to “build, train, and run” ranking models. *See* Ex. M ¶¶ 8, 22–23; Ex. N ¶¶ 11–16, 19. Except for emergency recovery procedures, no one at Google has access to the totality of the data and code stored in Google’s databases,¹⁵ and the systems used to interact with them. Ex. M ¶ 8; Ex. N ¶ 12. Even if Google could make all of those tools and systems available, Google cannot say with any degree of confidence that they can be configured (much less safely configured) with the particular analytical capabilities that Plaintiffs request.

To begin with, working with a particular system within Google’s Search, Ads, or Index infrastructure typically requires the direct involvement of the engineers who specialize in that system. Ex. M ¶ 24; Ex. N ¶¶ 20–21. To take RankEmbed as an example, no one at Google outside the handful of dedicated, experienced RankEmbed engineers has the knowledge and expertise to effectively experiment with and manipulate the RankEmbed model. Ex. N ¶ 21. As explained by a Senior Director of Engineering who is responsible for the quality of web results in Google Search and who has been working on the Google search ranking team for 13 years, if she wanted to conduct an experiment with respect to RankEmbed, she would need to consult with the

¹⁵ Google no longer maintains a single repository of all of its code, and has enacted additional security settings and fragmentation of its code into different repositories. Ex. M ¶ 25; Ex. N ¶ 12.

RankEmbed experts on her team who have a deeper understanding of the bespoke systems. *Id.* ¶¶ 20–21. And performing the engineering work to modify the code for such an experiment is only the first step. *Id.* ¶ 19. Access to the RankEmbed model code does not guarantee access to the necessary data to train the model, so additional access may need to be provisioned. *Id.* ¶¶ 12–14. Running the experiment would additionally require access to the compute resources needed to train the model and to run the experiment itself—resources that would exceed the compute quota of any one Google engineer. *See id.* ¶¶ 15–16. Finally, the new model would need to be served in production, which requires specific system access. *See Ex. N* ¶¶ 17–19. Even with access akin to what is provided to a senior Google engineer, it simply would not be possible to run a RankEmbed experiment without additional access requests and support from various Google engineers tailored to the specific project. For these reasons, Google cannot simply provide the Technical Committee with generalized access to run experiments or to build and train models. *See id.* ¶ 19.

Simply put, Google’s systems are not designed to provide access in the manner Plaintiffs have requested. *Ex. M* ¶¶ 22–23; *Ex. N* ¶ 10. Without specifying at the outset the scope and intent of the work the Technical Committee intends to perform, a generalized access plan may still result in Technical Committee Members and staff encountering difficulties accessing code, signals, logs, models, or compute resources implicated in the experiment or investigation they are trying to perform. *Ex. N* ¶¶ 11–19.

The final sentence of Plaintiffs’ proposal for Section 3.3 raises additional difficulties: It recites that “[c]onfigurations that render the environment review-only, or that prevent execution, querying, or simulation, are inconsistent with Section VII.A.7.d of the Final Judgment and shall not be imposed.” *Ex. A* § 3.3. While Google is committed to ensuring that the Technical Committee has the broad access afforded by the Final Judgment, this language introduces problematic

ambiguities. Google understands from its discussions with the Technical Committee (and as memorialized in correspondence from the Department of Justice), that the Technical Committee seeks read- and audit-oriented capabilities, not the ability to write changes to Google's code or alter Google's production stack. This sentence, however, appears to prohibit Google from making the data available outside a live environment. And taken literally, this sentence could allow the Technical Committee to access and modify code powering consumer-facing products. Google sees no reason why the Technical Committee would want (much less need) the ability to implement changes to consumer-facing products, and any request along those lines would raise a host of problems. Google accordingly sought clarification from Plaintiffs, but Plaintiffs refused to answer. Because the sentence is unworkable, overbroad, and seemingly inconsistent with the Technical Committee's intent, Google respectfully submits that it should be struck. The language to which Google has agreed confirms that Google will ensure the Technical Committee has the ability to execute queries against relevant datasets and that Google will make available "other Google-provided tools, software, ancillary data, and computational resources as are reasonably necessary to support the analytic work of the TC." Ex. B § 3.3.

Implementation difficulties aside, there are significant additional practical reasons why Google cannot make such broad access available. To begin with, the Court has concluded that the Technical Committee is an "enforcement arm of the government." *United States v. Google LLC*, 2025 WL 3496448, at *24 (D.D.C. Dec. 5, 2025). Opening up access without limitation would expose the Technical Committee members and staff to Google information consisting of intellectual property, including trade secrets; material protected by attorney-client privilege; information shared by third parties to which Google has promised confidentiality; and information about Google's numerous products and businesses that have nothing to do with Search, Search Text

Ads, or any other aspect of the Final Judgment. Merely granting signatories “access to Google[’s] corporate network” would gratuitously expose a considerable volume of information and systems. Ex. A § 3.2. There is no basis in the Final Judgment to compel such breathtakingly sweeping access at the outset: rather, the Final Judgment contemplates requests for “reasonable access.” ECF No. 1462 § VII.A.7.c.

Plaintiffs’ request for such sweeping access contravenes both Rule 65(d)’s specificity requirement, *see Schmidt v. Lessard*, 414 U.S. 473, 476–77 (1974), and the Fourth Amendment’s prohibition on unreasonable searches and seizures. Over a century’s worth of case law teaches that a federal enforcer cannot lawfully demand virtually unfettered access to a company’s records, even to investigate a violation of the law. “It is contrary to the first principles of justice to allow a search through all the respondents’ records, relevant or irrelevant, in the hope that something will turn up.” *Fed. Trade Comm’n v. Am. Tobacco Co.*, 264 U.S. 298, 306 (1924); *see also, e.g., In re Grand Jury Subpoena*, 828 F.3d 1083, 1088 (9th Cir. 2016). For that reason, an agency cannot issue a document subpoena or a civil investigative demand unless “(1) the inquiry is within the authority of the agency, (2) the demand is not too indefinite and (3) the information sought is reasonably relevant.” *Consumer Fin. Prot. Bureau v. Accrediting Council for Indep. Colleges & Schs.*, 854 F.3d 683, 688 (D.C. Cir. 2017) (cleaned up).

Antitrust remedial decrees are no exception. The Fourth Amendment requires a showing of relevance before granting federal enforcers access to a particular class of corporate records. *See, e.g., United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (noting that “a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power” and that “the inquiry [must be] within the authority of the agency, the demand [must] not [be] too indefinite and the information

sought [must be] reasonably relevant.”); *United States v. Bausch & Lomb Optical Co.*, 321 U.S. 707, 725–26 (1944) (holding that the Fourth Amendment permits “visitatorial powers” as part of an antitrust decree where reasonably necessary to effectuate the remedy). *United States v. Int’l Nickel Co. of Canada*, 203 F. Supp. 739 (S.D.N.Y. 1962), is instructive. There, the U.S. Department of Justice entered into a consent decree with the defendants to resolve Sherman Act claims. *Id.* at 740. The consent decree gave the government the right to inspect “records and documents” relating to any matters contained in the judgment. *Id.* A dispute soon arose over the implementation of that remedy—specifically, whether the government could be present during the selection of relevant records and documents for its review. The government argued that it “d[id] not want to see, inspect or copy all documents of the defendants,” but it *did* “want access to all such documents and files as are necessary to insure that all relevant documents have been produced.” *Id.* at 741. The Court rejected the government’s request. Noting the constitutional concerns and surveying case law from the Supreme Court and the D.C. Circuit, the district court explained that “[a]ll the cases emphasize that only production of documents relevant to the inquiry may be compelled,” and concluded that it was “[o]bvious[]” that “irrelevant documents may not be required to enable the demanding agency to determine what is relevant.” *Id.* at 743 (cleaned up). The same is true here: Plaintiffs and the Technical Committee might want broad access, but that puts the remedial cart before the constitutional horse.¹⁶ *See Am. Tobacco*, 264 U.S. at 305–06 (rejecting the FTC’s claim that the FTC Act gives it an “unlimited right of access to the respondents’ papers” to investigate violations

¹⁶ The fact that the Technical Committee members and their staff may not be traditional government employees changes nothing. The Court has described the Technical Committee as “the enforcement arm of the government,” *United States v. Google LLC*, 2025 WL 3496448, at *24 (D.D.C. Dec. 5, 2025) (cleaned up), and it is black-letter law that conduct by the “instrument” or the “agent” of the state implicates the Fourth Amendment, *see, e.g., Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971).

of the Act, reasoning that “[a]nyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire”).

In short, the broad scope of access that Plaintiffs propose opens up a thicket of logistical, constitutional, and information-security complexities. None of this is necessary. Google respectfully requests the Court enter Google’s proposed access provisions.

2. Pace of Fulfillment

Google also requests that the Court adopt Google’s language in Section 3.1, which provides that Google shall make requested material available within ten business days, and, if Google needs additional time, it shall so advise the Technical Committee within five business days of the request. Under Plaintiffs’ proposal, future requests for material would be required to be fulfilled in two business days. Again, Google understands the Technical Committee’s need for prompt access, but Google cannot commit in the abstract that it will be able to make any requested data or system available within two business days. As described in Heather Adkins’ Declaration, the time it takes to provision access to a given dataset or system depends on a number of factors, including the complexity of the request and the time necessary to understand the intent and desired outcome for the request, the amount of investigation necessary to understand the datasets and Google systems that are relevant to the request, the amount of correspondence necessary to determine who manages access to those datasets and systems, and the security controls, approvals, and access requirements associated with them. Ex. M ¶¶ 31–32; *see also* Ex. N ¶¶ 10–19, 22. In practical terms, that means Google may need to undertake substantial work upon receipt of a request. For example, a request for a particular class of data will require Google to ascertain which engineers work with that data set, to discuss with those engineers how the data can be collected, and to resolve any roadblocks

that may arise. Once that process concludes, even simple permission requests can take 24 hours (or more) to propagate to the system. While Google intends to provision the Technical Committee with access as expeditiously as it can, Google cannot promise that it can always occur within two business days.

B. Google Should Be Permitted to Approve the Removal of its Information from the Inspection Environment.

Google also respectfully requests that the Court permit a procedure through which a Google “clean team” may assess and sign off on requests to remove Google’s HSI and any derivative work product from the Inspection Environment.

One of the most significant concerns when designing an information-security framework is the potential for data removal. Ex. M ¶¶ 27–29. Once data is removed from its environment, the environment can no longer protect it. *Id.* ¶ 28. Information security specialists thus pay special attention to when and how data can flow out of the system to some other source. *Id.* In the modern agentic AI era, security vulnerabilities can be exploited at machine speed and autonomous AI agents can aggregate and stage sensitive data and intellectual property, making data loss prevention and pre-removal review procedures an increasingly important safeguard. *Id.* ¶ 30.

Google’s proposed framework accommodates the Technical Committee’s requirements while ensuring there are checks on the removal of Google’s sensitive information. Under Google’s proposal (Ex. B § 3.5), Google enables the removal of necessary materials from the Chromebook environment subject to review by an independent “Clean Team.” Composed of Google employees with no involvement in the remedies or the underlying litigation, a Clean Team would ensure oversight without exposing the Technical Committee’s work streams to litigation counsel and witnesses. Google’s framework additionally invites the Technical Committee to propose “additional qualifications or restrictions” for Clean Team members (Ex. B § 3.5.4). The Clean

Team’s review is strictly bounded: Requests may be denied solely upon “a good-faith belief that such request poses an unreasonable risk to the privacy of users, to Google’s security, or to Google’s intellectual property rights” (Ex. B § 3.5.5). In addition, to support time-sensitive needs and Court deadlines, the Clean Team is required to respond presumptively within five business days and to use best efforts to provide expedited responses upon reasonable request (Ex. B § 3.5.5).

Plaintiffs’ proposal, by contrast, offers none of the balance built into Google’s: It would give the Technical Committee, the Plaintiffs, and their staff an unqualified right to remove Google’s user data, algorithms, and source code from the Inspection Environment and place it in locations of their choosing. Such restrictionless exfiltration of Google data, algorithms, and source code poses an extraordinary vulnerability that could be compromised not just by human threats but also agentic AI threats, as illustrated by recent security incidents involving OpenAI and Hugging Face. Ex. M ¶ 30. Plaintiffs’ proposed absence of limitations also finds no basis in precedent. To the contrary, courts routinely issue protective orders sharply curtailing who may access source code and how. For example, the Northern District of California’s Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets requires that “[t]he source code shall be made available for inspection on a secured computer in a secured room without Internet access or network access to other computers”; prohibits the removal of source code from the inspection environment; and authorizes monitoring “to ensure that there is no unauthorized recording, copying, or transmission of the source code.” *See* § 9(c).¹⁷

Google appreciates that the Technical Committee’s work is fundamentally different from a standard litigation source code inspection. But the difference in posture does not mean a difference

¹⁷ The Northern District of California’s Model Protective Order is available at https://cand.uscourts.gov/sites/default/files/documents/ND_Cal_Patent_Highly_Sensitive_Model_Prot_Ord_Revised.pdf.

in risk, particularly in view of the broad access afforded to the Technical Committee. With that broad access comes the responsibility to collaborate with Google to ensure that robust protections are in place to minimize the risk of unintended harm to systems, user privacy, and intellectual property. Google respectfully submits that its proposal balances those considerations appropriately, and the Court should adopt it.

C. Plaintiffs’ Access to Google’s Highly Sensitive Information Should Be Subject to an Agreement Beyond the Existing Protective Order.

Google also respectfully requests that the Court order that Plaintiffs’ counsel and representatives who receive access to Google’s HSI be bound to the protections afforded by the Source Code Agreement. While Google does not object to the Plaintiffs receiving access to Google HSI, Google cannot agree to allow access in the absence of the same (or substantially similar) procedural safeguards as those that the Technical Committee will be held to.

Plaintiffs’ proposal to review Google HSI without any separate agreement (or supplemental protective order) presents unnecessary practical and legal risks. Source code is often described as a company’s “crown jewels,” and Google source code is some of the most sensitive intellectual property that exists at the company. “It is well recognized among lower courts that source code requires additional protections to prevent improper disclosure because it is often a company’s most sensitive and most valuable property.” *Drone Techs., Inc. v. Parrot S.A.*, 838 F.3d 1283, 1300 n.13 (Fed. Cir. 2016). Accordingly, courts routinely order even “extreme measures . . . to protect the[] confidentiality” of source code. *Via Vadis Controlling GmbH v. Skype, Inc.*, 2013 WL 646236, at *3 (D. Del. Feb. 21, 2013). And although this case is unique given its remedial posture, the security concerns surrounding the Source Code Agreement are *more* significant—not less—because it is not only Google’s source code at issue but also sensitive user data.

Plaintiffs have stated they will treat the materials removed from the Inspection Environment as Highly Confidential under the existing Protective Order. That Protective Order, however, is inadequate because it was not designed to address the concerns inherent in the access the Technical Committee will receive pursuant to the Source Code Agreement. The primary concern of the existing Protective Order is *what* the parties and their agents may access and *who* may be included in that process. *See* ECF No. 98. Although the Protective Order contains certain provisions touching on how eligible persons may access covered information—providing, for instance, that an in-house counsel’s document-review platform must be password protected—that was not the primary focus. Here, all parties recognize the importance of answering the question of *how* data is accessed. In that respect, the Source Code Agreement offers additional protections absent from even the higher tier of the Protective Order. For example, the Source Code Agreement limits access to Google HSI on a person-by-person basis, limits removal of Google HSI from the Inspection Environment, and (under Google’s proposal) includes a patent-prosecution bar. By contrast, the Protective Order permits unlimited reproduction of Highly Confidential material and broad dissemination among Plaintiffs’ attorneys, all without Google’s knowledge.

Given the highly sensitive character of Google HSI, the difference is of significant practical consequence. Under Plaintiffs’ proposal, nothing would stop the Plaintiffs from directly copying every line of Google’s source code made available to the Technical Committee and every byte of Google user data in the Technical Committee’s possession to the local computing environments of an unbounded number of employees of the fifty-three plaintiffs. Were one of those computing environments to be breached, it would be important for Google to understand whether its users’ data or its code or algorithms were compromised. Under Google’s proposal, Google would know who in each federal, state, municipal, or territorial attorney general office has received access.

Under Plaintiffs’ proposal, Google (and potentially Plaintiffs) would be in the dark. Ex. M ¶¶ 7–8, 27–29.

To be sure, Google does not mean to impugn the Plaintiffs’ record-keeping or data-security practices. But it is not enough to rely on individual employees’ desire to be good stewards of Google’s code and Google’s users’ data. Just last month, the U.S. Department of Justice informed the U.S. District Court for the District of New Jersey that DOJ attorneys had supplied Apple’s and other third parties’ data to a vendor in a manner that contravened the Federal Information Security Modernization Act. *See United States v. Apple Inc.*, No. 24-cv-4055, ECF No. 500, at 1–2 (D.N.J. Aug. 25, 2026).

When Google asked Plaintiffs why they were refusing to sign the Source Code Agreement, Plaintiffs cited ethical or legal constraints but declined to identify specific offending provisions. Google expects that there is a way to solve for their concerns. For instance, if Plaintiffs’ concern arises from the fact that the Source Code Agreement is a private contract, that problem can be solved by the Court entering a substantially similar protective order with Plaintiffs. On that score, Google notes that the federal government has previously entered into stipulated protective orders with special restrictions for source code. *See, e.g., Giesecke & Devrient GMBH v. United States*, No. 17-cv-1812, Dkt. No. 244 (Fed. Cl. Nov. 19, 2021) (protective order with source code tier applying to federal government); *Science Applications Int’l Corp. v. United States*, No. 17-cv-825, Dkt. No. 34 (Fed. Cl. May 8, 2018) (same); *Thales Visionix, Inc. v. United States*, No. 14-cv-513, Dkt. No. 79 (Fed. Cl. May 8, 2018) (same). Google is aware of no legal or ethical impediment that would preclude that approach. And as discussed above, Plaintiffs’ proposed alternative—i.e., sweeping government access to Google’s systems over Google’s objections—raises intractable legal concerns.

D. The Court Should Impose a Patent-Prosecution Bar.

Google also respectfully asks that the Court order a standard patent-prosecution bar to protect the trade-secret information the Technical Committee, its staff, and the Plaintiffs will access under the Source Code Agreement. The provision is important to ensure that persons who receive access to Google’s trade secrets will not use that knowledge when applying for a patent.

Patent-prosecution bars—routine features of protective orders in patent-infringement litigation—prohibit the recipient of sensitive intellectual property from pursuing a patent in a related field for a period of time.¹⁸ They operate as a prophylactic procedure designed to ensure that trade secrets revealed during litigation are not used (even inadvertently) to apply for intellectual property on behalf of another company or person. Courts order prosecution bars in a range of contexts beyond patent litigation where the nature of the litigation warrants one. *See, e.g., Biogen Inc. v. Neurimmune Holding AG*, No. 25-cv-11347, Dkt. No. 80 (D. Mass. Apr. 24, 2026) (breach of contract litigation); *AbbVie v. BeiGene Ltd.*, No. 24-cv-8167, Dkt. 50 (N.D. Ill. Feb. 12, 2025) (trade secret litigation); *In re Social Media Adolescent Addiction/Personal Injury Prods. Liab. Litig.*, 22-md-3047, Dkt. No. 1728 (N.D. Cal. Feb. 27, 2025) (personal injury litigation). As the U.S. Department of Justice explained in one criminal case where it successfully sought the imposition of a patent-prosecution bar, “patent prosecution bars are common in technology-related litigation.” United States of America’s Status Report, *United States v. Pani*, No. 08-CR-40034, Dkt. No. 70, at 3 (D. Mass. Mar. 1, 2010); *see also United States v. Pani*, 2010 WL 3928681, at *1

¹⁸ The U.S. District Court for the Northern District of California, for example—a court that hears a considerable number of software-related patent cases—includes an optional patent-prosecution bar provision in its template Protective Order. *See* Model Stipulated Protective Order For Litigation Involving Patents, Highly Sensitive Confidential Information And/Or Trade Secrets, § 8, *available at* https://cand.uscourts.gov/sites/default/files/documents/ND_Cal_Patent_Highly_Sensitive_Model_Prot_Ord_Revised.pdf.

(D. Mass. Oct. 4, 2010) (“[T]he Court notes that patent bars are not uncommon in cases involving valuable highly complex technical information.”).

Here, Google seeks a patent-prosecution bar prohibiting persons who receive access to Google HSI under the Source Code Agreement from applying for a patent in certain fields relating to the information they may receive. Ex. B § 9.¹⁹ The patent-prosecution bar would apply during the time that the Source Code Agreement signatory works with the Technical Committee and for two years afterwards.

To be clear, Google’s request for a patent-prosecution bar does not result from any distrust of the Technical Committee or its staff. Rather, patent-prosecution bars are entered in recognition of the fact that “it is very difficult for the human mind to compartmentalize and selectively suppress information once learned, no matter how well-intentioned the effort may be to do so.” *FTC v.*

Exxon Corp., 636 F.2d 1336, 1350 (D.C. Cir. 1980); *accord In re Deutsche Bank Tr. Co. Americas*, 605 F.3d 1373, 1378 (Fed. Cir. 2010); *see also* Scott L. Garland, *Eenie, Meenie, Miney, Mo:*

Choosing and Working With an Expert in a Stolen Trade Secrets Case, Cyber Investigative Issues II in U.S. Attorneys’ Bulletin, at 72 (Mar. 2014), *available at*

<https://www.justice.gov/sites/default/files/usao/legacy/2014/04/11/usab6202.pdf> (Patent

prosecution bars are common precisely because “[r]elying on [an] expert to mentally quarantine any litigation-derived information from his or her other professional activities could be futile.”).

If any member of the Technical Committee or their dozens of staff wish to file a patent application

¹⁹ Those areas are query understanding, information retrieval, web search indexing, or crawling, web spam detection, ranking of web results or ad results, search or search ad syndication, digital ad auctions and pricing, machine learning, large language models, artificial intelligence (including but not limited to generative artificial intelligence functionality trained for, adapted for, or used in connection with web search), or privacy-preserving search technologies. Ex. B § 9.

in a field relating to, e.g., “ranking of web results,” they cannot forget what they will have learned from Google’s HSI.

Google’s proposed patent-prosecution bar satisfies the test typically used in patent-infringement litigation where a prosecution bar is sought. More specifically, “the information designated to trigger the bar, the scope of activities prohibited by the bar, the duration of the bar, and the subject matter covered by the bar” should all “reasonably reflect the risk presented by the disclosure of proprietary competitive information.” *In re Deutsche Bank Tr. Co. Americas*, 605 F.3d at 1381. That the information to be made available via the Source Code Agreement contains sensitive intellectual property is not in dispute. The scope of activities prohibited by the bar is standard fare and appears nearly verbatim in a range of other protective orders.²⁰ The duration of the bar extends two years after conclusion of the signatory’s work with the Technical Committee. And the subject matter of the bar is tailored to the proprietary information that the Technical Committee may solicit or receive, where the risk of competitive harm to Google is especially great. Finally, the bar is consistent with the Final Judgment, which already contemplates restrictions on the post-employment activities of the Technical Committee Members and their staff. *See* ECF No. 1462 § VII.A.2.c (prohibiting Technical Committee members from seeking employment from “Competitors” as defined by the Final Judgment for one year after service on the Technical Committee, absent the consent of the Parties); *see also* ECF No. 1543.

²⁰ Compare, e.g., Ex. B § 9 (“For purposes of this paragraph, ‘prosecution’ includes any activity related to (i) the preparation or prosecution (for any person or entity) of patent applications, including among others reexamination and reissue applications or (ii) directly or indirectly participating, drafting, amending, advising, or otherwise affecting the scope or maintenance of patent claims.”), with *Kolon Indus., Inc. v. Hyosung Advanced Materials Corp.*, No. 24-cv-415, Dkt. No. 80, § 14 (C.D. Cal. Sept. 26, 2024) (“For purposes of this Section, ‘prosecution’ includes any activity related to (i) the preparation or prosecution (for any person or entity) of patent applications, including among others reissue applications or (ii) directly or indirectly participating, drafting, amending, advising, or otherwise affecting the scope or maintenance of patent claims.”).

Google expects based on the parties' conferrals that Plaintiffs might argue that it is inappropriate to apply a prosecution bar to government lawyers or their staff. If so, that argument is incorrect. When the U.S. government is sued for patent infringement, for instance, its lawyers, staff, and experts are routinely subject to patent-prosecution bars. *See, e.g., Giesecke & Devrient GMBH v. United States*, No. 17-cv-1812, Dkt. No. 244 (Fed. Cl. Nov. 19, 2021) (protective order with prosecution bar applying to federal government); *Science Applications Int'l Corp. v. United States*, No. 17-cv-825, Dkt. No. 34 (Fed. Cl. May 8, 2018) (same); *Thales Visionix, Inc. v. United States*, No. 14-cv-513, Dkt. No. 79 (Fed. Cl. May 8, 2018) (same).

To the extent Plaintiffs' objection is based on a concern that the prosecution bar could hamper the recruitment of prospective Technical Committee staff, that too is no answer. Streamlining the hiring process cannot justify the prosecution of patents based on Google's trade secrets. "[A] patent prosecution bar may be necessary and right" even if "hiring an outside expert might be complicated by the need to find one willing to forgo patent prosecution in the relevant area." Scott L. Garland, *Eenie, Meenie, Miney, Mo: Choosing and Working With an Expert in a Stolen Trade Secrets Case*, Cyber Investigative Issues II in U.S. Attorneys' Bulletin, at 74 (Mar. 2014).

Dated: September 16, 2026

Respectfully submitted,

/s/ Karl E. Herrmann

Claire M. Maddox (D.C. Bar #498356)

Travis R. Chapman (D.C. Bar #90031151)

Danielle Hauck

Grant M. Fergusson (D.C. Bar #90004882)

Karl E. Herrmann (D.C. Bar #1022464)

Ryan T. Karr

Emma Waitzman (D.C. Bar #1738427)

U.S. Department of Justice

Antitrust Division

Technology & Digital Platforms Section

450 Fifth Street NW, Suite 7100

Washington, DC 20530

Telephone: (202) 549-7155

Claire.Maddox@usdoj.gov

Counsel for Plaintiff United States of America

By: /s/ Amanda Wentz
Amanda J. Wentz
Assistant Attorney General
Office of the Arkansas Attorney General
101 West Capitol Avenue
Little Rock, Arkansas 72201
Phone: (501) 682-1178
Amanda.Wentz@ArkansasAG.gov

Counsel for Plaintiff State of Arkansas

By: /s/ Carolyn D. Jeffries
Rob Bonta, Attorney General
Paula Blizzard, Senior Assistant Attorney General
Michael Jorgenson, Supervising Deputy Attorney General
Brian Wang, Deputy Attorney General
Carolyn D. Jeffries, Deputy Attorney General (DC Bar No. 1600843)
Office of the Attorney General
California Department of Justice
455 Golden Gate Avenue, Suite 11000
San Francisco, California 94102
Cari.Jeffries@doj.ca.gov

Counsel for Plaintiff State of California

By: /s/ Lee Istrail
James Uthmeier, Attorney General
R. Scott Palmer, Special Counsel, Complex Enforcement Chief, Antitrust Division
Lee Istrail, Assistant Attorney General
Office of the Attorney General, State of Florida
PL-01 The Capitol
Tallahassee, Florida 32399
Lee.Istrail@myfloridalegal.com
Scott.Palmer@myfloridalegal.com

Counsel for Plaintiff State of Florida

By: /s/ Charles Thimmesch
Christopher Carr, Attorney General
Logan B. Winkles, Deputy Attorney General
Ronald J. Stay, Jr., Senior Assistant Attorney General
Charles Thimmesch, Senior Assistant Attorney General
Office of the Attorney General, State of Georgia
40 Capitol Square, SW
Atlanta, Georgia 30334-1300
cthimmesch@law.georgia.gov

Counsel for Plaintiff State of Georgia

By:
/s/ Scott L. Barnhart
Theodore Edward Rokita, Attorney General
Scott L. Barnhart, Chief Counsel and Director, Consumer Protection Division
Office of the Attorney General, State of Indiana
Indiana Government Center South, Fifth Floor
302 West Washington Street
Indianapolis, Indiana 46204
Scott.Barnhart@atg.in.gov

Counsel for Plaintiff State of Indiana

By: /s/ Jonathan E. Farmer
Russell Coleman, Attorney General
J. Christian Lewis, Commissioner of the
Office of Consumer Protection
Philip R. Heleringer, Executive
Director of the Office of Consumer
Protection
Jonathan E. Farmer, Deputy Executive
Director of the Office of Consumer
Protection
Office of the Attorney General,
Commonwealth of Kentucky
1024 Capital Center Drive, Suite 200
Frankfort, Kentucky 40601
Philip.Heleringer@ky.gov

*Counsel for Plaintiff
Commonwealth of Kentucky*

By: /s/ Asyl Nachabe
Liz Murrill, Attorney General
Asyl Nachabe, Assistant Attorney General
Office of the Attorney General, State of
Louisiana
Public Protection Division
909 Poydras St. Suite 1850
New Orleans, LA 70112
(225) 326-6435
NachabeA@ag.louisiana.gov

Counsel for Plaintiff State of Louisiana

By: /s/ Scott Mertens
Dana Nessel, Attorney General
Scott Mertens, Assistant Attorney General
Michigan Department of Attorney General
P.O. Box 30736
Lansing, Michigan 48909
MertensS@michigan.gov

Counsel for Plaintiff State of Michigan

By: /s/ Alison Esbeck
Alison Esbeck
Assistant Attorney General
Missouri Attorney General's Office
815 Olive Street | Suite 200
Saint Louis, Missouri 63101
Alison.esbeck@ago.mo.gov
Phone: 314-340-4977

Counsel for Plaintiff State of Missouri

By: /s/ Anna Schneider
Anna Schneider
Special Assistant Attorney General,
Senior Counsel,
Montana Office of Consumer Protection
P.O. Box 200151
Helena, MT 59602-0150
Phone: (406) 444-4500
Anna.schneider@mt.gov

Counsel for Plaintiff State of Montana

By: /s/ Mary Frances Jowers
Alan Wilson, Attorney General
W. Jeffrey Young, Chief Deputy
Attorney General
C. Havird Jones, Jr., Senior Assistant
Deputy Attorney General
Mary Frances Jowers, Assistant Deputy
Attorney General
Office of the Attorney General
State of South Carolina
1000 Assembly Street
Rembert C. Dennis
Building
P.O. Box 11549
Columbia, South Carolina 29211-1549
mfjowers@scag.gov

Counsel for Plaintiff State of South Carolina

By: /s/ Diamante Smith

Ken Paxton, Attorney General
Brent Webster, First Assistant Attorney
General
Ralph Molina, Deputy First Assistant
Attorney General
William D. Wassdorf, Deputy Attorney
General for Civil Litigation
Thomas York, Division Chief, Antitrust
Division
Diamante Smith, Assistant Attorney
General, Antitrust Division
Office of the Attorney General,
State of Texas
P.O. Box 12548
Austin, Texas 78711-2548
(512) 936-1162
Diamante.Smith@oag.texas.gov

Counsel for Plaintiff State of Texas

By: /s/ Caitlin M. Madden

Joshua L. Kaul, Attorney General
Caitlin M. Madden, Assistant
Attorney General
Wisconsin Department of Justice
17 W. Main St.
Post Office Box 7857
Madison, Wisconsin 53707-7857
caitlin.madden@Wisconsin.gov

Counsel for Plaintiff State of Wisconsin

PHILIP WEISER

Attorney General of Colorado

/s/ Jonathan B. Sallet

Jonathan B. Sallet, DC Bar No. 336198

Steven M. Kaufmann

Elizabeth W. Hereford

Conor J. May

Colorado Office of the Attorney General

1300 Broadway, 7th Floor

Denver, CO 80203

Telephone: (720) 508-6000

E-Mail: Jon.Sallet@coag.gov

Steve.Kaufmann@coag.gov

Elizabeth.Hereford@coag.gov

Conor.May@coag.gov

William F. Cavanaugh, Jr.

PATTERSON BELKNAP WEBB &
TYLER LLP

1133 Avenue of the Americas

New York, NY 10036

Telephone: (212) 336-2793

E-Mail: wfcavanaugh@pbwt.com

Counsel for Plaintiff State of Colorado

MIKE HILGERS

Attorney General of Nebraska

Justin C. McCully, Assistant Attorney
General

Nebraska Department of Justice

Office of the Attorney General

2115 State Capitol

Lincoln, NE 68509

Telephone: (402) 471-9305

E-Mail: Justin.mccully@nebraska.gov

William F. Cavanaugh, Jr.

PATTERSON BELKNAP WEBB &
TYLER LLP

1133 Avenue of the Americas

New York, NY 10036

Telephone: (212) 336-2793

E-Mail: wfcavanaugh@pbwt.com

Counsel for Plaintiff State of Nebraska

KRISTIN K. MAYES

Attorney General of Arizona

Robert A. Bernheim, Unit Chief Counsel

Jayne Weber, Senior Litigation Counsel

Arizona Office of the Attorney General

400 West Congress, Ste. S-215

Tucson, Arizona 85701

Telephone: (520) 628-6507

E-Mail: Robert.Bernheim@azag.gov

Jayne.Weber@azag.gov

Counsel for Plaintiff State of Arizona

BRENNA BIRD

Attorney General of Iowa

Noah Goerlitz, Assistant Attorney General

Office of the Attorney General of Iowa

1305 E. Walnut St., 2nd Floor

Des Moines, IA 50319

Telephone: (515) 725-1018

E-Mail: Noah.goerlitz@ag.iowa.gov

Counsel for Plaintiff State of Iowa

LETITIA JAMES

Attorney General of New York

Elinor R. Hoffmann

Morgan J. Feder

Michael D. Schwartz

Office of the New York State Attorney
General

28 Liberty Street

New York, NY 10005

Telephone: (212) 416-8513

E-Mail: Elinor.hoffmann@ag.ny.gov

Morgan.feder@ag.ny.gov

Michael.schwartz@ag.ny.gov

Counsel for Plaintiff State of New York

JEFF JACKSON
Attorney General of North Carolina

Kunal Janak Choksi
Joshua Daniel Abram
North Carolina Department of Justice
114 W. Edenton St.
Raleigh, NC 27603
Telephone: (919) 716-6000
E-Mail: kchoksi@ncdoj.gov
jabram@ncdoj.gov

Counsel for Plaintiff State of North Carolina

JONATHAN SKRMETTI
Attorney General of Tennessee

J. David McDowell
Austin Ostiguy
Tyler Corcoran
Office of the Attorney General and Reporter
P.O. Box 20207
Nashville, TN 37202
Telephone: (615) 741-8722
E-Mail: David.McDowell@ag.tn.gov
austin.ostiguy@ag.tn.gov
Tyler.Corcoran@ag.tn.gov

Counsel for Plaintiff State of Tennessee

DEREK E. BROWN
Attorney General of Utah

Marie W.L. Martin, Division Director
Utah Office of Attorney General
160 E 300 S, 5th Floor
P.O. Box 140811
Salt Lake City, Utah 84114
Telephone: (801) 440-9825
E-Mail: mwmartin@agutah.gov

Counsel for Plaintiff State of Utah

STEPHEN J. COX
Attorney General of Alaska

Jeff Pickett
Senior Assistant Attorney General
State of Alaska, Department of Law
Office of the Attorney General
1031 W. Fourth Avenue, Suite 200
Anchorage, Alaska 99501
Telephone: (907) 269-5275
E-Mail: Jeff.pickett@alaska.gov

Counsel for Plaintiff State of Alaska

WILLIAM TONG
Attorney General of Connecticut

Nicole Demers
Office of the Attorney General of Connecticut
165 Capitol Avenue, Suite 5000
Hartford, CT 06106
Telephone: (860) 808-5202
E-Mail: Nicole.demers@ct.gov

Counsel for Plaintiff State of Connecticut

KATHLEEN JENNINGS
Attorney General of Delaware

Michael Andrew Undorf
Delaware Department of Justice
Fraud and Consumer Protection Division
820 N. French St., 5th Floor
Wilmington, DE 19801
Telephone: (302) 683-8816
E-Mail: Michael.undorf@delaware.gov

Counsel for Plaintiff State of Delaware

BRIAN SCHWALB
Attorney General of the District of Columbia

Elizabeth Gentry Arthur
Office of the Attorney General for the

District of Columbia
400 6th Street NW
Washington, DC 20001
Telephone: (202) 724-6514
E-Mail: Elizabeth.arthur@dc.gov

Counsel for Plaintiff District of Columbia

DOUGLAS MOYLAN
Attorney General of Guam

Norman Lee Miller, Jr.
Office of the Attorney General of Guam
590 S. Marine Corps Drive, Suite 901
Tamuning, Guam 96913
Telephone: (671) 475-2710
E-Mail: nmillerjr@oagguam.org

Counsel for Plaintiff Territory Guam

ANNE E. LOPEZ
Attorney General of Hawai'i

Rodney I. Kimura
Department of the Attorney General, State
of Hawai'i
425 Queen Street
Honolulu, HI 96813
Telephone (808) 586-1180
E-Mail: Rodney.i.kimura@hawaii.gov

Counsel for Plaintiff State of Hawai'i

RAÚL LABRADOR
Attorney General of Idaho

John K. Olson
Office of the Idaho Attorney General
Consumer Protection Division
954 W. Jefferson St., 2nd Floor
P.O. Box 83720
Boise, ID 83720
Telephone: (208) 332-3549
E-Mail: John.olson@ag.idaho.gov

Counsel for Plaintiff State of Idaho

KWAME RAOUL
Attorney General of Illinois

Elizabeth Maxeiner
Brian Yost
Jennifer Coronel
Office of the Attorney General of Illinois
115 S. LaSalle St.
Chicago, IL 60603
Telephone: (773) 590-7935
E-Mail: Elizabeth.maxeiner@ilag.gov
Brian.yost@ilag.gov
Jennifer.coronel@ilag.gov

Counsel for Plaintiff State of Illinois

KRIS W. KOBACH
Attorney General of Kansas

Christopher Teters
Kansas Office of the Attorney General
120 S.W. 10th Avenue, 2nd Floor
Topeka, KS 66612
Telephone: (785) 296-3751
E-Mail: chris.teters@ag.ks.gov

Counsel for Plaintiff State of Kansas

AARON M. FREY
Attorney General of Maine

Christina M. Moylan
Office of the Attorney General of Maine
6 State House Station
August, ME 04333
Telephone: (207) 626-8800
E-Mail: Christina.moylan@maine.gov

Counsel for Plaintiff State of Maine

ANTHONY G. BROWN
Attorney General of Maryland

Schonette J. Walker
Melissa English

Office of the Attorney General of
Maryland
200 St. Paul Place, 19th Floor
Baltimore, MD 21202
Telephone: (410) 576-6480
E-Mail: swalker@oag.state.md.us
menglish@oag.state.md.us

Counsel for Plaintiff State of Maryland

ANDREA CAMPBELL
Attorney General of Massachusetts

Jennifer E. Greaney
Office of the Attorney General of
Massachusetts
One Ashburton Place, 18th Floor
Boston, MA 02108
Telephone: (617) 963-2981
E-Mail: Jennifer.greaney@mass.gov

*Counsel for Plaintiff Commonwealth of
Massachusetts*

KEITH ELLISON
Attorney General of Minnesota

Zach Biesanz
Senior Enforcement Counsel
Office of the Minnesota Attorney General
Antitrust Division
445 Minnesota Street, Suite 600
St. Paul, MN 55101
Telephone: (651) 757-1257
E-Mail: Zach.biesanz@ag.state.mn.us

Counsel for Plaintiff State of Minnesota

AARON D. FORD
Attorney General of Nevada

Michelle C. Badorine
Lucas J. Tucker
Nevada Office of the Attorney General
100 N. Carson Street
Carson City, NV 89701

Telephone: (775) 684-1164
E-Mail: mbadorine@ag.nv.gov
ltucker@ag.nv.gov

Counsel for Plaintiff State of Nevada

JOHN FORMELLA
Attorney General of New Hampshire

Brandon Garod
Office of Attorney General of New
Hampshire
1 Granite Place South
Concord, NH 03301
Telephone: (603) 271-1217
E-Mail: Brandon.h.garod@doj.nh.gov

*Counsel for Plaintiff State of New
Hampshire*

JENNIFER DAVENPORT
Acting Attorney General of New Jersey

Yale A. Leber
Abiola G. Miles
Deputy Attorneys General
New Jersey Attorney General's Office
25 Market Street, P.O. Box 106
Trenton, NJ 08625
Telephone: (609) 376-2383
E-Mail: Yale.Leber@law.njoag.gov
Abiola.Miles@law.njoag.gov

Counsel for Plaintiff State of New Jersey

RAÚL TORREZ
Attorney General of New Mexico

Judith E. Paquin Cholla Khoury
Assistant Attorney General
New Mexico Office of the Attorney
General
408 Galisteo St.
Santa Fe, NM 87504
Telephone: (505) 490-4885
E-Mail: jpaquin@nmag.gov

ckhoury@nmag.gov

Counsel for Plaintiff State of New Mexico

DREW WRIGLEY
Attorney General of North Dakota

Elin S. Alm
Assistant Attorney General
Consumer Protection and Antitrust
Division
Office of the Attorney General of North
Dakota
1720 Burlington Drive, Suite C
Bismarck, ND 58504
Telephone: (701) 328-5570
E-Mail: ealm@nd.gov

*Counsel for Plaintiff State of North
Dakota*

D. ANDREW WILSON
Attorney General of Ohio

Beth Ann Finnerty, Section Chief,
Antitrust
Sarah Mader, Assistant Attorney General,
Antitrust
Office of the Attorney General of Ohio
30 E Broad Street, 26th Floor
Columbus, OH 43215
Telephone: (614) 466-4328
E-Mail: Beth.Finnerty@ohioago.gov
Sarah.Mader@ohioago.gov

Counsel for Plaintiff State of Ohio

GENTNER DRUMMOND
Attorney General of Oklahoma

Cameron R. Capps
Office of the Oklahoma Attorney General
313 NE 21st Street
Oklahoma City, OK 73105
Telephone: (405) 522-0858
E-Mail: Cameron.capps@oag.ok.gov

Counsel for Plaintiff State of Oklahoma

DAN RAYFIELD
Attorney General of Oregon

Gina Ko, Assistant Attorney General
Oregon Department of Justice
100 SW Market Street
Portland, OR 97201
Telephone: (503) 934-4400
E-Mail: Gina.Ko@doj.oregon.gov

Counsel for Plaintiff State of Oregon

DAVID W. SUNDAY, JR.
Attorney General of Pennsylvania

Tracy W. Wertz
Joseph S. Betsko
Pennsylvania Office of Attorney General
Strawberry Square
Harrisburg, PA 17120
Telephone: (717) 787-4530
E-Mail: jrbetsko@attorneygeneral.gov
twertz@attorneygeneral.gov

*Counsel for Plaintiff Commonwealth of
Pennsylvania*

LOURDES L. GÓMEZ TORRES
Secretary of Justice

TANIA L. FERNÁNDEZ-MEDERO
Assistant Secretary of Justice

SAMUEL WISCOVITCH-CORALI
Deputy Undersecretary

Pablo Tufiño-Soto
Senior Attorney
Antitrust Division
Puerto Rico Department of Justice
P.O. Box 9020192
San Juan, Puerto Rico 00902-0192
Telephone: (787) 721-2900, Ext. 1205

E-Mail: ptufino@justicia.pr.gov

Counsel for Plaintiff Territory Puerto Rico

PETER NERONHA
Attorney General of Rhode Island

Stephen Provazza
Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
Telephone: (401) 274-4400
E-Mail: SProvazza@riag.ri.gov

Counsel for Plaintiff State of Rhode Island

MARTIN J. JACKLEY
Attorney General of South Dakota

Yvette K. Lafrentz
Office of the Attorney General of South Dakota
1302 E. Hwy 14, Suite 1
Pierre, SD 57501
Telephone: (605) 773-3215
E-Mail: Yvette.lafrentz@state.sd.us

Counsel for Plaintiff State of South Dakota

CHARITY R. CLARK
Attorney General of Vermont

Christopher J. Curtis, Assistant Attorney General
Office of the Attorney General of Vermont
109 State St.
Montpelier, VT 05609
Telephone: (802) 828-3170
E-Mail: christopher.curtis@vermont.gov
Counsel for Plaintiff State of Vermont

JAY JONES

Attorney General of Virginia

Tyler T. Henry
Senior Assistant Attorney General
Antitrust Unit
Office of the Attorney General of Virginia
202 N. 9th Street
Richmond, VA 23219
Telephone: (804) 692-0485
E-Mail: thenry@oag.state.va.us

Counsel for Plaintiff State of Virginia

NICHOLAS W. BROWN
Attorney General of Washington

Amy N.L. Hanson
Senior Managing Assistant Attorney General
800 Fifth Avenue, Suite 2000
Seattle, WA 98104
Telephone: (206) 464-5419
E-Mail: Amy.hanson@atg.wa.gov

Counsel for Plaintiff State of Washington

JOHN B. McCUSKEY
Attorney General of West Virginia

Douglas Lee Davis
Office of the Attorney General, State of West Virginia
1900 Kanawha Boulevard East
Building 6, Suite 401
P.O. Box 1789
Charleston, WV 25305
Telephone: (304) 558-8986
E-Mail: Douglas.l.davis@wvago.gov

Counsel for Plaintiff State of West Virginia

KEITH KAUTZ
Attorney General of Wyoming

William T. Young

Wyoming Attorney General's Office
2320 Capitol Avenue
Kendrick Building
Cheyenne, WY 82002
Telephone: (307) 777-7847
E-Mail: William.young@wyo.gov

Counsel for Plaintiff State of Wyoming

WILLIAMS & CONNOLLY LLP

By: /s/ John E. Schmidtlein

John E. Schmidtlein (D.C. Bar No. 441261)
Benjamin M. Greenblum (D.C. Bar No. 979786)
Colette T. Connor (D.C. Bar No. 991533)
680 Maine Avenue, SW
Washington, DC 20024
Tel: 202-434-5000
jschmidtlein@wc.com
bgreenblum@wc.com
cconnor@wc.com

WILSON SONSINI GOODRICH & ROSATI P.C.

Michael Sommer (admitted *pro hac vice*)
Franklin M. Rubinstein (D.C. Bar No.
476674) 1700 K Street, NW
Washington, DC 20006
Tel: 202-973-880
msommer@wsgr.com
frubinstein@wsgr.com

ROPES & GRAY LLP

Mark S. Popofsky (D.C. Bar No.
454213) 2099 Pennsylvania Avenue,
NW Washington, DC 20006
Tel: 202-508-4624
Mark.Popofsky@ropesgray.com

Matthew McGinnis (admitted *pro hac*
vice) Prudential Tower
800 Boylston Street
Boston, MA 02199
Tel: 617-951-7703
Matthew.McGinnis@ropesgray.com

Counsel for Defendant Google LLC