No. 25-521

IN THE

Supreme Court of the United States

GOOGLE LLC, ET AL.,
Petitioners,

v.

EPIC GAMES, INC.,
Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF OF *AMICUS CURIAE* THE CENTER FOR CYBERSECURITY POLICY AND LAW IN SUPPORT OF PETITION FOR *CERTIORARI*

SARAH L. SCOTT
VENABLE LLP
750 E. Pratt St.
Suite 900
Baltimore, MD 21202

ELIZABETH C. RINEHART
Counsel of Record
JENNIFER C. DASKAL
J. DANIEL EVERSON
VENABLE LLP
600 Mass. Ave., NW
Washington, DC 20001
LCRinehart@Venable.com

Counsel for Amicus Curiae

November 5, 2025

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Center for Cybersecurity Policy and Law ("Center") is a nonprofit organization that develops, advances, and promotes best practices for ensuring cybersecurity and protecting public safety as a result.[2] Its interest is in safeguarding the security of mobile computing and protecting against measures that introduce new vulnerabilities into connected devices used by billions of people worldwide. It has particular concerns about the security and public safety risks that arise from the injunction imposed in this case, which could make it easier for cyber-criminal and nation-state adversaries to target millions of Android phone users. As a nonprofit organization that has studied mobile phone security and is dedicated to advancing cybersecurity best practices, the Center is uniquely positioned to provide insight into the security considerations relevant to the injunction being reviewed in this case.[3]

---

[1] No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus curiae* or their counsel made a monetary contribution to this brief's preparation or submission.

[2] Petitioner Google is a member of the Center. Google has paid general dues for its membership and has contributed financially to specific Center projects, including over the last year. Google has not contributed any money that was intended to fund the preparation or submission of this brief.

[3] *See* Center for Cybersecurity Policy and Law, *Trusted App Stores: Protecting Security and Integrity* 3 (Feb. 2024), https://tinyurl.com/TrustedAppStore [hereinafter "Center, *Trusted App Stores*"]; Center for Cybersecurity Policy and Law, *Mobile Future: Pathways to Continued Improvement in Mobile Security and*

INTRODUCTION AND SUMMARY OF ARGUMENT

The district court injunction introduces significant security risks into the mobile device ecosystem, which were not adequately considered by the Ninth Circuit. The Center is specifically concerned about the parts of the injunction that require Google to: (i) immediately allow developers to provide link-outs to external websites for app downloads, *see* App. 69a, ¶ 10; (ii) provide third-party app stores access to the Google Play Store's entire app catalog, without regard to whether or how these third-party app stores protect against copy-cat apps or address needed security updates (the "catalog-access provision," App. 69a–70a, ¶ 11); and (iii) enable the distribution of third-party app stores on the Google Play Store, with screening measures limited to only those which are "strictly necessary and narrowly tailored" (the "app-store-distribution" provision, App. 70a, ¶ 12).[4] These measures fail to account for the growing sophistication and prevalence of malicious cybercriminals and nation-state adversaries, the important security measures that Google currently has in place to mitigate these threats, the ways in which these requirements will force Google to undo some of those security measures, and the risks that will result.

Privacy 3 (May 2021), https://tinyurl.com/MobileFuturePDF [hereinafter "Center, *Mobile Future*"].

[4] The Center's brief focuses on the security risks resulting from ¶¶ 9–12 of the injunction, and the inadequacy of the proposed Technical Committee to sufficiently address these risks (¶ 13). App. 69a–71a. It does not take a position on the provisions restricting Google from certain revenue-sharing and payment agreements.

The risks to user security—and broader public safety—are not hypothetical. Mobile devices provide a treasure trove of information about their users, including information about a user's friends and family, financial information, and physical location. Mobile devices also contain passkeys or other tokens that can be used to access enterprise systems, exposing sensitive business information and government data.[5] Studies indicate that mobile malware has grown in sophistication and frequency over time—with tens of thousands of new types of malware detected daily.[6]

Yet, despite the significance of the threat, the risks to user security and public safety were not sufficiently considered by either the Ninth Circuit or district court opinions. The Ninth Circuit never acknowledged the security risks associated with the required link-out provision, failed to adequately consider the security costs associated with the catalog-access provision, and presumed, without support, that Google can address the app-store distribution measures with simple technical measures. In so doing, the Ninth Circuit seems to have adopted the district court's assumption that the security risks posed by the injunction are

---

[5] *See, e.g.,* David Klepper, *Chinese hackers and user lapses turn smartphones into a 'mobile security crisis'*, Associated Press (June 8, 2025), https://tinyurl.com/KlepperAPNews; Jim Coyle, *As Government's Mobile Usage Grows, So Do Cyberthreats*, FedTech (Feb. 2, 2025), https://tinyurl.com/FedTechCoyle (describing risks that foreign threat actors can use mobile device infiltration as a means to steal federal employee credentials and infiltrate government networks).

[6] *See* Jannatul Ferdous et al., *A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms*, 11 IEEE Access 121118, 121118, 121124 (Oct. 30, 2023), https://tinyurl.com/FerdousReview (examining trends and compiling studies).

insubstantial and readily manageable, and that those that do exist can readily be addressed by a Technical Committee. This is an incorrect assumption.

Moreover, the Ninth Circuit seems to have rested its opinion on a flawed assumption that because Apple and Google operate differently, with Apple providing a "walled garden" and Google allowing for "open distribution," Google does not meaningfully invest in or compete on security.[7] This also is incorrect. Google has invested heavily in the security architecture underlying its Google Play Store, in developing and imposing security requirements on developers that distribute their apps through Google Play, and in security vetting for both apps and updates to apps.[8] These measures have demonstrable benefits. It is not accidental that Android users who used app stores other than Google Play are up to nineteen times more likely

---

[7] *Epic Games, Inc. v. Google LLC*, No. 24-6256, 2025 WL 2167402, at *7 (9th Cir. July 31, 2025). The Ninth Circuit cites from Google's opening brief for the proposition that "Android's open philosophy offers users and developers wider choices" than iOS does, which "limit[s] Google's ability to directly protect users from encountering malware and security threats when they download apps." But the panel omits the next critical sentence: "*Google has designed and operated Play to ensure Android users have a secure, trusted environment to obtain apps and in-app content*, which is an essential component of consumer satisfaction with a mobile device and key to keeping Android as a robust competitor to Apple." Appellants' Opening Br. at 1–2 (emphasis added). As the omitted sentence explains, Google recognizes the security risks created by its more open approach and increased choice and operates Google Play in ways designed to minimize those risks.

[8] *See* Kleidermacher Decl. (Oct. 11, 2024), Ninth Circuit Excerpts of Record 2-ER-205, 206, 210 ¶¶ 2, 6, 20 [hereinafter "Kleidermacher Decl."]; *infra* notes 22–28.

to come across malicious apps than those who used Google Play.[9]

By ignoring the benefits of Google's security protections and discounting the security risks created by link-outs, unvetted apps, and catalog-access requirements, the injunction risks decreasing security for millions of Android users and the enterprise systems, including business and government systems, that users access through their phones. Moreover, these are not risks that can simply be shifted to users—without broader costs to the security of the digital ecosystem. Most users lack the knowledge and skills to protect themselves from sophisticated malware and use of fraudulent, but seemingly credible links.[10] Users may also believe that they are "invulnerable" to security risks, thinking that malware happens to someone else.[11] In implementing security vetting and reviews, Google operates as first-line defense against malicious applications and links. Measures that require Google to water down or limit the scope of its security review will expose vulnerabilities that can, given the interconnections between devices and broader networks with which those devices are connected, propagate through multiple enterprises and systems.

---

[9] Platon Kotzias, Juan Caballero, & Leyla Bilge, *How Did That Get In My Phone? Unwanted App Distribution on Android Devices*, IEEE Symposium on Sec. & Priv. 2 (Oct. 20, 2020), https://tinyurl.com/PlatonKotziasEtAl [hereinafter, "Kotzias et al."].

[10] *See* Center, *Trusted App Store* at 9-10; Center, *Mobile Future* at 10–11.

[11] *See* Marthie Grobler, Raj Gaire, & Surya Nepal, *User, Usage and Usability: Redefining Human Centric Cyber Security*, Frontiers in Big Data 4 (Mar. 9, 2021), https://tinyurl.com/MarthieGrobler.

The Court should grant the petition in order to fully consider and remedy the security risks created by the district court's injunction.

ARGUMENT

A. Both the Ninth Circuit and District Court Fail to Account for Google's Existing Security Measures and Incorrectly Assume That the Security Risks Created by the Injunction Are Marginal and Easily Manageable

The Ninth Circuit fails to account for the rising and increasing sophistication of cybersecurity threats, the fact that mobile phones are a particularly attractive attack vector, and the importance of strong security in order to protect user security and public safety. It also discounts the importance of security measures that Google has in place and thus discounts the security risks that result from the district court's injunction. In so doing, it repeats key errors in the district court's reasoning—namely, the assumption that the security risks resulting from the injunction are marginal and easily manageable.

The Ninth Circuit seems to assume that, because Google operates a more open mobile operating system than Apple, Google does not meaningfully compete on security. Such an assumption ignores Google's investment in the security of the Google Play Store—and the concrete results. Among other measures, Google imposes security requirements on developers and extensively vets all of the apps and updates distributed through the Google Play Store.[12] As a result, Google

---

[12] *See infra* notes 22–28.

has created a more secure user experience for Google Play users than offered through other Android app stores. Google Play users rely on this additional security and safety.[13] In sum, Google operates a more open mobile operating system than Apple *and* meaningfully competes on security.

Thus, even assuming, *arguendo*, the Ninth Circuit has correctly identified the relevant market as limited to Android app stores, security remains an important pro-competitive force within this market. The injunction risks significantly undercutting the security protections that help keep users safe.

B. The Current and Evolving Threat Environment Should Be Considered

Over the past decade, cyber threats have increased dramatically in both frequency and scale. Malicious actors take advantage of the growing number of vulnerabilities in systems and networks to intentionally cause harm, disrupt operations, steal sensitive data,

---

[13] *See* Cesar Daniel Barreto, *The Hidden Risks of Sideloading: Why You Should Stick to Official App Stores*, Security Briefing (June 13, 2025), https://tinyurl.com/CesarDanielBarreto (noting that the risk of malware is reduced on Google Play as compared to third-party app stores); Center, *Trusted App Stores* at 9–12 (describing the challenges users face in effectively addressing mobile security risks and the importance of centralized controls to protect user safety); Center, *Mobile Future* at 7–10 (same).

and undermine trust.[14] And these actors are increasingly targeting mobile systems.[15]

Nation-state actors and their proxies pose a particularly acute threat, as they have become increasingly sophisticated and aggressive in their efforts to exploit vulnerabilities in the digital ecosystem.[16] Financially motivated cyber criminals also represent a growing threat, with ransomware actors increasing in scope and sophistication—aided in significant part by the ability to target identified victims. The FBI's Internet Crime Complaint Center reports year-over-year increases in financial losses from scams.[17] The estimated global cost of cybercrime is projected to rise by over $6.4 trillion between now and 2029, reaching a staggering $15.6 trillion over the next four years.[18]

---

[14] *See* World Econ. F., *Global Cybersecurity Outlook 2025* 4 (Jan. 13, 2025), https://tinyurl.com/GlobalCybersecurityOutlook (noting that the cybercriminals are exploiting the vulnerabilities created by the rapid adoption of emerging technologies with increasing sophistication and scale).

[15] *See* Shubham, Rajinder Singh Sodhi, & Preet Kaur, *Safeguarding mobile ecosystems: A comprehensive examination of cyber-attacks and mobile security*, 5 Int'l J. Multidisciplinary Trends 34 (2023), https://tinyurl.com/ShubhamEtAl (warning that "[c]yber-attacks targeting mobile devices have become increasingly prevalent and diverse, posing substantial risks to individuals, organizations, and even nations").

[16] *See, e.g.,* Off. Dir. Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community* 11–12 (Mar. 25, 2025), https://tinyurl.com/ODNIReport.

[17] Fed. Bureau of Investigation, *Internet Crime Report 2024* 7, 10 (Apr. 23, 2025), https://tinyurl.com/FBIInternetCrimeReport.

[18] Peter A. Jensen, *Estimated cost of cybercrime worldwide 2018–2029 (in trillion U.S. dollars)*, Biocomm AI (July 30, 2024), https://tinyurl.com/PeterAJensen.

Mobile phones are an increasingly common target of attack.[19] This is not surprising. After all, a single malicious app can provide access to all of the personal, financial, and business data on one's phone, as well as sensitive geolocation data. Links that download malicious software can be used to embed malware on phones—enabling the collection of sensitive personal information like contacts, call logs, location history, and browser activity, which can then be exploited for identity theft or surveillance. Mobile devices' constant connectivity and integration with enterprise systems amplify the scale of potential damage well beyond an individual user. Attackers can, and do, use access to mobile devices to gain access to organizational networks, confidential corporate information, and sensitive government systems—posing serious threats to informational security, national security, and public safety.

Despite these risks, the mobile ecosystem has remained relatively secure, as compared to other areas of cybersecurity.[20] This resilience is largely the result of careful, deliberate efforts by platform providers and app store operators, including both Google and Apple, who have invested heavily in designing complex, multilayered security systems to protect users from a wide

---

[19] *See* Timur Mirzoev et al., *Mobile Application Threats and Security*, 2 World of Comput. Sci. & Info. Tech. J. 1 (Feb. 2025), https://tinyurl.com/TimurMirzoevEtAl (warning that "[m]obile devices have become a big target for cyber criminals"); Global Anti-Scam Alliance, *Global State of Scams – 2023* 2 (2023), https://tinyurl.com/GlobalStateofScams (indicating that some 78% of mobile users encountered at least one phishing scam in 2023).

[20] *See* Center, *Mobile Future* at 3 (describing findings of cybersecurity experts).

range of threats.[21] The district court's injunction risks unraveling some of these key security measures and thus putting users at risk.

C. Importance of Google's Current Vetting Measures and Security Controls

Google has implemented multi-layered security and privacy-protective features that differentiate Google Play from that of other app stores available to Android users. Among other measures, Google imposes several security requirements on developers that distribute their apps through Google Play. In order to be available in the Play Store, apps and app updates must meet specified security standards and best practices.[22] Google requires that all apps and app updates pass a centralized vetting process involving both machine based detection and human reviews before they are allowed to appear in the Play Store.[23] Google

---

[21] *See infra* notes 22–28; Center, *Trusted App Stores* at 10–12 (describing security measures).

[22] *See* Zak Doffman, *Google Play Store Low-Quality App Purge—Also Delete From Your Phone*, Forbes (Sept. 17, 2024), https://tinyurl.com/ForbesDoffman (describing efforts Google has been taking to improve app security); Bill Toulas, *Google Play will enforce business checks to curb malware submissions*, Bleeping Computer (July 13, 2023), https://tinyurl.com/BleepingComputerToulas (same); Google, *Android Security Paper 2024* 40 (2024), https://tinyurl.com/AndroidSecurityPaper [hereinafter, "*Android Security Paper*"].

[23] Bethel Otuteye, Khawaja Shams, & Ron Aquino, *How we kept the Google Play & Android app ecosystems safe in 2024*, Google Security Blog (Jan. 29, 2025), https://tinyurl.com/GoogleSecurityBlog; *Cloud-based protections*, Google Play Protect (last updated Oct. 31, 2024), https://tinyurl.com/GooglePlayProject (describing the analysis and review process for all applications); *see also* Kleidermacher Decl. ¶¶ 2, 6, 20; Center, *Trusted*

supplements these measures with Google Play Protect, a built-in security feature on Android devices that scans all apps for malware and other potentially harmful software.[24] To further protect against the distribution of unvetted and thus potentially insecure apps, Google disallows developers from using Google Play to distribute third-party app stores.[25]

Thanks to these multi-layered security requirements and reviews, Google has created a relatively secure user environment, as compared to most other Android app stores.[26] A 2020 study found that "other top alternative markets" available to Android users were five times riskier on average, and users were up to nineteen times more likely to come across malware or a malicious app than those who used the Google Play Store.[27] Another study found that 99.9% of mobile malware was hosted on third-party app stores, as opposed to first-party app stores like Google Play and the Apple App Store.[28]

The panel decision largely ignores the important security measures currently in place and thus fails to appreciate the ways in which the injunction's

---

App Stores at 11 (describing security measures that Google has put in place).

[24] *Android Security Paper* at 37.

[25] *See Google Play Developer Distribution Agreement,* Google Play ¶ 4.5 (Feb. 5, 2024), https://tinyurl.com/GooglePlayAgreement.

[26] *See* Yuta Ishii et al., *Understanding the Security Management of Global Third-Party Android Marketplaces*, ACM SIGSOFT Int'l Workshop 6 (Sept. 5, 2017), https://tinyurl.com/YutaIshii; *see also* Center, *Trusted App Stores* at 8.

[27] Kotzias et al., at 2.

[28] Symantec, *Internet Security Threat Report* 50–52 (Mar. 2018), https://tinyurl.com/SymantecReport2018.

requirements will undercut digital security and heighten risks to users.

D. Exposing Users to Unvetted External Links Creates Significant Security Risks

The injunction adds new insecurity into the mobile ecosystem by requiring Google to allow all developers to embed links in their apps that enable users to download apps from outside the app store. Such links can create significant security and privacy vulnerabilities.[29] Malicious actors may, for example, employ links to take users to websites that appear legitimate but in fact are designed to deceive—prompting users to disclose sensitive credentials or download malicious software onto their devices. Even links that are intended to take users to legitimate sites can be hijacked so that a user is instead redirected to what turns out to be a malicious site, albeit while still looking legitimate and thus deceiving users into sharing payment information or downloading a harmful application.[30]

The widespread use of dynamic links exacerbates these concerns. Unlike static links, which are fixed and unchanging, dynamic links are designed to change based on real-time inputs, including user-specific data such as location, login status, session history, or other identifiers. Thus, even if Google were in a position to perform security reviews of the link-outs to external apps that this injunction would allow, the

---

[29] *See* Center, *Trusted App Stores* at 9–11 (describing security risks of sideloading and how first-party app stores combat these threats); Kleidermacher Decl. ¶¶ 6–7.

[30] *See* Yutian Tang et al., *All Your App Links Are Belong to Us: Understanding the Threats of Instant Apps Based Attacks*, Ass'n for Computing Mach. 914, 916 (Nov. 8, 2020), https://tinyurl.com/YutianTang.

benefits of any such vetting would be minimal to non-existent. Because the destination of a dynamic link may vary with each user or session, pre-vetting cannot sufficiently protect user safety and security. Malicious actors exploit the variability created by dynamic links to redirect traffic to compromised sites, harvest personal data, or inject malware—all without the user realizing anything has changed.

Exacerbating the risks, dynamic URLs often use query strings—information appended to the URL—to determine what information will be conveyed to the user. Query strings can carry tracking tokens, usernames, email addresses, and other personal identifiers that users may not intend to disclose or even know that they are sharing.[31] When exposed to third parties or logged in browser history, this information can be used to obtain personal, private information about users, track them across services, or link their online activities without their knowledge or consent.

The requirement that Google permit all developers to use link-outs to downloadable apps runs counter to the advice of multiple government agencies, including the National Security Agency,[32] Commerce Department,[33] the Department of Homeland Security's

---

[31] *See* Andrew G. West & Adam J. Aviv, *On the Privacy Concerns of URL Query Strings*, IEEE CS Sec. & Priv. Workshops 1 (2014), https://tinyurl.com/AndrewGWestEtAl.

[32] Nat'l Sec. Agency, *Mobile Device Best Practices* 1 (Oct. 2020), https://tinyurl.com/NSABestPractices.

[33] Christopher Brown et al., *Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue (Draft) NISTIR 8144* 8–10 (Sept. 2016), https://tinyurl.com/NISTAssessingThreat.

Cybersecurity and Infrastructure Security Agency,[34] and multiple foreign government security agencies[35] that advise against downloading apps from unvetted, external websites. By ignoring this expert input and requiring that Google allow such links, the injunction creates new insecurities for users.

E. Malicious Actors Are Likely to Exploit the Required Catalog-Sharing Provision

Requiring Google to make available its app catalog for use on unvetted app stores creates a new playing field for malicious actors, thereby creating a new set of security risks. Malicious actors can easily set up a shell third-party "store" and populate it with apps from Google Play in order to give it a veneer of credibility, yet also include malicious, deceptive, or pirated apps. Malicious actors can also populate app stores with what appear to be Google Play apps, but are in fact deceptively modified copycats that, once downloaded, introduce malware on the user's phone.[36]

The catalog-sharing provision also fails to account for the need for security updates to address newly discovered security vulnerabilities. Google routinely disseminates such updates through Google Play.[37] While

---

[34] Cybersecurity & Infrastructure Sec. Agency, *Capacity Enhance Guide: Mobile Device Cybersecurity Checklist for Organizations* (Nov. 2021), https://tinyurl.com/CISANov2021.

[35] *See* Center, *Trusted App Stores* at 8–9 (compiling a list of such warnings from international partners, including the United Kingdom, India, New Zealand, and Europol).

[36] *See* Center, *Trusted App Stores* at 9–11; Center, *Mobile Future* at 7–8.

[37] *See, e.g.,* Jon Gilbert, *5 critical reasons why keeping your android security updates current is more important than ever*, Android Police (July 5, 2025), https://tinyurl.com/AndroidPolice-

Google could still provide needed updates to third-party app stores, Google would have no control over whether those app stores then push these security updates to their users. Worse, malicious actors could pose as Google or another legitimate developer and send malicious code to third-party app store users in the guise of an official update, without any way for users to verify whether or not the update is legitimate.

Even the opt-out provision for the subset of developers who do not want their apps distributed on other app stores creates room for exploitation. A malicious actor might identify this gap to develop a copy-cat app that tricks users into thinking it is the otherwise "missing" app—yet is instead used to download malware onto users' phones. In fact, copy-cat apps are a very common feature—or more accurately, bug—of third-party app stores. [38] Users are not likely to be in a position to know which developers opted in and which opted out—and are thus vulnerable to deception, particularly if the app is presented in a way that matches the version offered in Google Play.

The injunction seeks to address these concerns by giving Google eight months to create and implement the technology necessary to comply with this provision. But there is no technological solution to the user-confusion risks identified here.

SecurityUpdates ("Every Android phone receives monthly security updates until the end of its software support life cycle . . . Security updates protect your phone from hackers by removing exploits, patching bugs, and fixing vulnerabilities.")

[38] Kotzias et al., at 3.

F. The Required App-Store Distribution Provision Increases the Security Risks

The required app-store distribution provision will require Google to host app stores that provide limited-to-no curation or security vetting of their apps or developers. Even worse, it will give malicious app stores that intentionally distribute malware a new platform for distribution—on what has historically been the relatively secure Google app store.

To address these risks, the injunction gives Google leeway to develop "reasonable" security and technical measures to protect users from the risks posed by potentially malicious apps distributed on its Play Store.[39] But it limits such security measures to those that Google can establish are "strictly necessary" and "narrowly tailored."[40] As with the prior provision, it gives Google eight months to develop these measures—even though Google's expert stated that it would need twelve to sixteen months to put in place baseline security requirements.[41]

Even with sufficient time to establish new security measures, the requirement that such measures be "strictly necessary" and "narrowly tailored" risks limiting action, in a way that is ultimately underinclusive given the nature of the threat. Threat actors are increasingly sophisticated and constantly evolving. Good security measures do not just react to already known and existent threats. Such measures need to anticipate and respond to prospective threats,

---

[39] Permanent Injunction, App. 70a, ¶ 12.

[40] *Id.*

[41] Baccetti Decl. (June 24, 2024), Ninth Circuit Excerpts of Record 2-ER-386, ¶ 36.

including threats that may not (and hopefully do not) come to fruition. Google, however, is likely to face challenges in establishing that these kinds of anticipatory and inherently prophylactic security measures are "strictly necessary" and "narrowly tailored," given that they are forward-looking, seeking to ward off threats that have not yet occurred.[42]

G. Core Security Decisions with Profound Implications for Digital Security Should Not Be Delegated to an Unaccountable Technical Committee

The injunction's creation of a three-person "Technical Committee" to review disputes related to security fails to adequately address the significant security risks created by the injunction. Per the injunction, one member of this Technical Committee is to be recommended by Google, another by Epic, and the third chosen by these first two members. There are no required qualifications for serving on the Committee. And there is no overarching guidance about how much weight to give security considerations. If the Technical Committee cannot resolve an issue, either party may submit the issue for resolution to the court.[43]

The security consequences of insufficient vetting or controls are simply too important and too complex to relegate to committee decision-making. Moreover, the likelihood that the committee will be in a position to objectively evaluate the core security considerations is further undermined by the fact that the committee members are to be appointed by parties adverse to each other, in active litigation, and with

---

[42] *See* Kleidermacher Decl. ¶¶ 23–28.

[43] Permanent Injunction, App. 71a, ¶ 13.

differing business interests and approaches to innovation.[44] In short, the "Technical Committee" proposal is a completely unrealistic solution to the serious security risks created by the district court's injunction that risks compounding the burden of the injunction. This Committee is being asked to make core decisions about security, with wide-ranging implications for user and public safety, but without any accountability to the broader public.

CONCLUSION

The equitable remedies imposed in this case create significant security risks that were not sufficiently addressed by the Ninth Circuit opinion. *Amicus* urges this Court to grant the petition for *certiorari*.

Dated: November 5, 2025

ELIZABETH C. RINEHART
Counsel of Record
JENNIFER C. DASKAL
J. DANIEL EVERSON
VENABLE LLP
600 Massachusetts Ave. NW
Washington, DC 20001
Tel: (202) 344-4698
LCRinehart@Venable.com

SARAH L. SCOTT
VENABLE LLP
750 E. Pratt St.
Suite 900
Baltimore, MD 21202

[44] *Id.*