Nos. 24-6256, 24-6274, 25-303

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

EPIC GAMES, INC.,
Plaintiff-Appellee,
v.
GOOGLE LLC, ET AL.,
Defendants-Appellants.

On Appeal from the United States District Court
for the Northern District of California
Nos. 3:20-cv-05671-JD, 3:21-md-02981-JD
Hon. James Donato

BRIEF OF *AMICUS CURIAE* THE CENTER FOR CYBERSECURITY POLICY AND LAW IN SUPPORT OF DEFENDANTS-APPELLANTS

Jennifer C. Daskal
Sarah L. Scott
VENABLE LLP
600 Massachusetts Ave, NW
Washington, DC 20001
(202) 344-8281
jdaskal@venable.com
slscott@venable.com

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, counsel for the Center for Cybersecurity Policy and Law ("Center") states:

Amicus curiae the Center is a section 501(c)(6) nonprofit organization. It has no parent corporations, and no publicly held corporation has a 10 percent or greater ownership interest in the Center.

/s/ *Jennifer C. Daskal*
Jennifer C. Daskal

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Rules

Other Authorities

I. STATEMENT OF IDENTITY AND 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 will 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 Pursuant to Fed. R. App. P. 29(a)(4)(E), *amicus* certifies that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money intended to fund preparing or submitting the brief; and no person—other than the amicus, its members, or its counsel—contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

2 Defendant-Appellant 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 Privacy* 3 (May 2021), https://tinyurl.com/MobileFuturePDF [hereinafter "Center,

II. SUMMARY OF ARGUMENT

The district court injunction introduces significant security risks into the mobile device ecosystem, which were not adequately considered by the panel below. The Center is specifically concerned about the parts of the injunction that require Google to: (i) immediately allow all developers to provide link-outs to external websites for app downloads, *see* 1-ER-4, ¶ 10; (ii) provide third-party app stores access to Google Play Store's entire app catalog, without regard to whether or how these third-party apps protect against copy-cat apps or address needed security updates (the "catalog-access provision," 1-ER-4–5, ¶ 11); and (iii) enable the distribution of third-party app stores on the Google Play Store, with screening measures limited to only that which is "strictly necessary and narrowly tailored" (the "app-store-distribution" provision, 1-ER-5, ¶ 12).[4] Collectively, 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, and their relative effectiveness in doing so, as compared to other app stores.

The risks to user security—and broader public safety—are not hypothetical.

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). 1-ER-4-5. It does not take a position on the provisions restricting Google from certain revenue-sharing and payment agreements.

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. It is not surprising that mobile devices have long been a target for malicious actors—a trend that has only increased over time.[5]

Yet, despite the significance of the threat, the risks to user security and public safety were not sufficiently considered by either the panel court or district court opinion. The panel opinion never acknowledged the security risks associated with the required link-out provision, failed to adequately consider the security considerations related to the catalog-access provision, and presumed, without support, that Google can address the app-store distribution measures with simple technical measures and reasonable fees. In so doing, the panel seems to have adopted the district court's assumption that the security risks posed by the injunction are insubstantial and readily manageable, and that those that do exist can readily be

5 *See* David Klepper, *Chinese hackers and user lapses turn smartphones into a 'mobile security crisis'*, Associated Press (June 8, 2025), https://tinyurl.com/KlepperAPNews; 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/JannatulFerdousEtAl (noting that tens of thousands of "new types of malware are discovered daily" and emphasizing the specific ways in which "mobile malware has grown significantly in sophistication and frequency").

addressed by a Technical Committee. This is an incorrect assumption.

Moreover, the panel opinion 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.[6] 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.[7] These measures have demonstrable benefits. As just one measure, Android users who used app stores other than Google Play are reportedly up to nineteen times more likely to come across malicious apps than those who used Google Play.[8]

---

6 *Epic Games, Inc. v. Google LLC*, No. 24-6256, 2025 WL 2167402, at *7 (9th Cir. July 31, 2025). The panel 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.

7 *See* Kleidermacher Decl. (Oct. 11, 2024), 2-ER-205, 206, 210 ¶¶ 2, 6, 20 [hereinafter "Kleidermacher Decl."]; *infra* notes 20–23.

8 Platon Kotzias, Juan Caballero, & Leyla Bilge, *How Did That Get In My*

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. The court should grant the petition for either rehearing *en banc* or panel rehearing, in order to fully consider the security risks created by the district court's injunction.

III. ARGUMENT

A. Both the Panel Court 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 panel court's ruling discounts the security measures that Google has in place and thus the security risks that result from the district court's injunction. The panel court also 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. 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

---

Phone? Unwanted App Distribution on Android Devices, IEEE Symposium on Sec. & Priv. 2 (Oct. 20, 2020), https://tinyurl.com/PlatonKotziasEtAl [hereinafter, "Kotzias et al."].

marginal and easily manageable.

The panel also 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 the ways in which Google has invested heavily 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.[9] As a result, Google 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.[10] In sum, Google operates a more open mobile operating system than Apple *and* meaningfully competes on security.

Thus, even assuming, *arguendo*, the panel has correctly identified the relevant market as limited to Android app stores, security remains an important pro-competitive force within this market.[11] The injunction risks significantly

---

9 *See infra,* notes 20–23.

10 *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).

11 The Center agrees with Google that the market definition affirmed in *Epic v. Apple*, 67 F. 4th 946, 981 (9th Cir. 2023)—namely the market for mobile gaming apps that includes Apple, Google, and other Android app stores—should also govern

undercutting the security protections that help keep users safe.

B. The Current and Evolving Threat Environment

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, and undermine trust.[12] And these actors are increasingly targeting mobile systems.[13]

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.[14] Financially motivated cyber criminals also represent a growing threat, with ransomware actors increasing in scope and

---

Epic's case against Google. *See* Appellant's Pet. for Reh'g at 11–15. That said, even if the market is limited to mobile gaming *within* the Android system, security is a critically important element of this market and distinguishes Google Play from other app stores available on the Android system.

12 *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).

13 *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").

14 *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.

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.[15] 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.[16]

Mobile phones are an increasingly common target of attack.[17] 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 use access to mobile devices to gain access to organizational

---

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

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

17 *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).

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.[18] 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 range of threats.[19] 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 be modeled for at least Android 13, which encourages developers to adopt strong security standards and best practices.[20] Google also requires that all apps and app updates pass a centralized

---

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

19 *See infra,* notes 20–23; *see also* Center, *Trusted App Stores* at 10–12 (describing security measures).

20 Google, *Android Security Paper 2024* 40 (2024),

and rigorous vetting process before they are allowed to appear in the Play Store.[21] The vetting process combines human security experts and machine-based threat detection to ensure all new apps are compliant with Play's security requirements.[22] To further protect users from unvetted, insecure apps, Google disallows developers from using Google Play to distribute third-party app stores.[23] Google 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] Google reports that, as a result of its multi-layered review process, it has banned more than 158,000 bad developer accounts that attempted to publish harmful apps.[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

---

https://tinyurl.com/AndroidSecurityPaper [hereinafter, "*Android Security Paper*"].

21 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 [hereinafter, "Otuteye et al."]; *see also* Center, *Trusted App Stores* at 11 (describing security measures that Google has put in place).

22 *See 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.

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

24 *Android Security Paper* at 37.

25 Otuteye et al.

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 these important security measures, and thus fails to appreciate the ways in which the injunction's 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. But links that take users to third-party websites in order to download unvetted apps create security and privacy vulnerabilities.[29] Such websites may appear legitimate but in fact are designed to

---

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.

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

deceive—prompting users to disclose sensitive credentials or download malicious software onto their devices. External links can also be hijacked so that a user is redirected to what is meant to be a legitimate site, but instead turns out to be a malicious site, 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 initial security reviews of the many link-outs to external apps that this injunction would allow, such vetting would be of little-to-no value. Because the destination of a dynamic link may vary with each user or session, such links cannot be pre-vetted. Malicious actors can 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 also often use query strings—information appended to the URL—to determine what information will be conveyed

---

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.

to the user. Query strings can also 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 also runs counter to the advice of multiple governments and private organizations that advise against downloading apps from unvetted, external websites.[32] By 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 makes it easier for malicious actors to operate, thereby creating a new set of security risks. Malicious actors can easily set up a shell third-party "store" and

---

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 *See Government Experts In The U.S.: Don't Sideload*, Trusted Future (June 24, 2022), https://tinyurl.com/TrustedFuture (compiling reports from U.S. government agencies emphasizing the importance of trusted app stores and recommending against downloading from third-party app stores); Center, *Trusted App Stores* at 8–9 (compiling a list of such warnings from international partners).

populate it with apps from Google Play, alongside malicious, deceptive, or pirated content. Malicious actors can also populate existing app stores with slightly modified versions of Google Play apps—that, once downloaded, introduce malware on the user's phone. As documented by prior Center research, users are not equipped to make the kind of fine-tuned assessments needed to distinguish legitimate and illegitimate apps, and they should not be expected to do so.[33]

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. While 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. Consider what happens when a developer decides to opt out of their app being made available to other app stores. A malicious actor might identify this gap to develop a copy-cat app that closely resembles the original application yet is used to download malware onto

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

users' phones. In fact, copy-cat apps are a very common feature (or more accurately, bug) of third-party app stores. [34] Users are unlikely to know that the developer has opted out of third-party distribution and will likely presume it is an app vetted by Google.

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.

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. To address these risks, the injunction gives Google leeway to develop "reasonable" security and technical measures to protect users. [35] But it limits such security measures to those that Google can establish are "strictly necessary" and "narrowly tailored," [36] and gives Google just eight months

34 Kotzias et al., at 3.
35 Permanent Injunction, 1-ER-5, ¶ 12.
36 *Id*.

to develop these measures, even though Google's expert stated that it would need twelve to sixteen months to do so.[37]

Even with a full year, providing appropriate security for third-party app stores hosted in the Play Store will be difficult, if not impossible. Good security measures are not just reactive measures narrowly tailored to a known threat. Such measures need to anticipate and respond to prospective threats, including threats that may not (and hopefully do not) come to fruition. Google, however, is likely to face challenges in establishing that prophylactic security measures are "strictly necessary" and "narrowly tailored," given that they are in anticipation of threats that have not yet occurred.[38]

G. Core Security Decisions with Profound Implications for Digital Security Should Not Be Delegated to a Yet-To-Be-Established and 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

37 Baccetti Decl. (June 24, 2024), 2-ER-386, ¶ 36.
38 *See* Kleidermacher Decl. ¶¶ 23–28.

security considerations. If the Technical Committee cannot resolve an issue, either party may submit the issue for resolution to the court.[39]

The security consequences of insufficient vetting or controls are simply too important and too complex to relegate to committee decision-making, let alone to a committee that has not yet been stood up. 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 is to be appointed by parties adverse to each other, in active litigation, and with differing business interests and approaches to innovation.[40] 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 yet-to-be established 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.

IV. CONCLUSION

The equitable remedies imposed in this case create significant security risks that were not sufficiently addressed by the panel opinion. This court should grant either the petition for rehearing *en banc* or panel rehearing and ultimately vacate the

39 Permanent Injunction, 1-ER-5–6, ¶ 13.
40 *Id.*

district court's injunction.

Dated: August 25, 2025

Respectfully submitted,

/s/ *Jennifer C. Daskal*

Jennifer C. Daskal
Sarah L. Scott
VENABLE LLP
600 Massachusetts Ave., N.W.
Washington, DC 20001

Counsel for Amicus Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

9th Cir. Case Number(s) 24-6256, 24-6274, 25-303

I am the attorney for *amicus curiae* The Center for Cybersecurity Policy and Law.

This brief contains 4,177 words, including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties.
- [ ] a party or parties are filing a single brief in response to multiple briefs.
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature */s/ Jennifer C. Daskal* **Date** August 25, 2025

CERTIFICATE OF SERVICE

I certify that on August 25, 2025, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system, which will send a notice of electronic filing to all counsel of record who have consented to electronic notification.

Dated: August 25, 2025

/s/ *Jennifer C. Daskal*
Jennifer C. Daskal

Counsel for Amicus Curiae