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 a Final Judgment of the United States
District Court for the Northern District of California (Donato, J.),
Nos. 3:20-cv-05671 & 3:21-md-02981

BRIEF OF *AMICI CURIAE* FORMER NATIONAL SECURITY OFFICIALS AND SCHOLARS IN SUPPORT OF DEFENDANTS-APPELLANTS' PETITION FOR REHEARING EN BANC AND/OR PANEL REHEARING

Roy T. Englert, Jr.
Ariel N. Lavinbuk
Shikha Garg
HERBERT SMITH FREEHILLS
KRAMER (US) LLP
2000 K Street NW, 4th Floor
Washington, DC 20006
(202) 775-4500
roy.englert@hsfkramer.com
ariel.lavinbuk@hsfkramer.com
shikha.garg@hsfkramer.com

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

Amici are former officials and scholars with decades of experience in cybersecurity and national security. They have served at senior levels for Presidents of both parties and played an outsized role in the creation of modern national security law and policy. They have devoted decades to protecting national security and ensuring that cybersecurity threats are minimized to the greatest extent possible consistent with the laws of the United States. *Amici* write to offer the Court their informed perspective on the national security disruptions that would result if this Court does not grant rehearing.

INTRODUCTION AND SUMMARY

The district court's injunction, upheld by a panel of this Court, risks creating massive cybersecurity vulnerabilities in the online ecosystem. At the heart of that risk is the injunction's requirement that Google collaborate with one company, Appellee in this case, to create a "Technical Committee" to control day-to-day operations of a platform with millions of apps used by millions of people every day.

The district court and the Technical Committee are woefully ill-equipped to manage the complex, numerous, and dynamic cybersecurity threats to millions of

---

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amici* certify that no person or entity, other than *amici* or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

Android users that will result from allowing countless new apps to flood the Google Play Store and third-party app stores. Google, with state-of-the-art cybersecurity practices and a trusted app ecosystem, is best positioned to manage those security risks, but the injunction would hamstring Google's ability to secure its platforms by requiring it to allow developers to provide links directly to users, to distribute third-party app stores, and to allow third-party app stores access to the Google Play Store catalog. Even one mis-clicked link or one nefarious downloaded app can have catastrophic results, allowing malicious actors to access Android devices and data.

The district court's remedy goes well beyond the red line the Supreme Court endorsed in the seminal case *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398 (2004). Quoting Professor Phillip Areeda, Justice Scalia's opinion for the Court warned that "[n]o court should impose a duty to deal that it cannot explain or adequately and reasonably supervise. The problem should be deemed irremediable by antitrust law when compulsory access requires the court to assume the day-to-day controls characteristic of a regulatory agency." *Id.* at 410-11, 415 (alteration marks omitted) (quoting Phillip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 852-53 (1989)).

Amici are concerned that Appellee appears to be misreading *Trinko* in an attempt to convince this Court not to grapple with this unprecedented remedy. Opp. to Mot. to Stay Injunction (Dkt. 218) at 23. In addition to addressing antitrust liability

(which Appellee acknowledges), *Trinko* states a limit to a court's power to order remedies in antitrust cases. Indeed, to emphasize the limitations of court-ordered remedies in antitrust cases, the Supreme Court also quoted the "equitable decree" the plaintiff sought there and observed that "[a]n antitrust court is unlikely to be an effective day-to-day enforcer of these detailed sharing obligations." 540 U.S. at 415. Yet in this case the panel upheld an injunction of vastly greater complexity than detailed sharing obligations. Ordering creation of a "Technical Committee" to satisfy extraordinary cybersecurity challenges that will inevitably flow from its remedies in this case clearly crosses the red line established in *Trinko*.

As national security experts, *amici* can shed light on the injunction's impact on national security, cybersecurity, and the public interest to show why the Court should grant rehearing to ensure that the district court's injunction does not put the cybersecurity of millions of Americans at risk.

ARGUMENT

I. THE INJUNCTION WILL CREATE NATIONAL-SECURITY RISKS

The injunction in part requires Google to give third-party app stores access to the entire Google Play catalog and to distribute third-party app stores through the Google Play Store itself.[2] Although it permits Google to "take reasonable measures

[2] Dkt. 1017 ¶¶ 11-12.

to ensure that the platforms or stores, and the apps they offer, are safe from a computer systems and security standpoint," Google must show that its security measures are "strictly necessary and narrowly tailored."[3] Those determinations can be vetoed by a three-person Technical Committee or the district court. Though Google and *amici* raised concerns that the Technical Committee's oversight was insufficient to protect users' security, the panel declined to engage meaningfully with this issue and upheld the injunction. Op. 64-65.

That was incorrect, and the injunction could be catastrophic for the Nation's security. Under the injunction, Google will have to distribute third-party app stores through the Google Play Store, and Google's ability to screen those app stores for security concerns is limited by the injunction. Given the speed at which large volumes of app stores could appear and the complex and varied security risks each app could pose, the Technical Committee—which will be predisposed to view any measures as a potential threat to competition—and district court are unlikely to be able to move quickly enough to protect users from grave threats.

These threats are far from hypothetical. Hostile nations and other malicious actors increasingly target Americans through app-based attacks. Because the injunction limits Google's ability to protect Android users, as soon as the injunction

[3] *Id.* ¶ 12.

goes into effect, they will be more vulnerable to cyberattacks, threatening both their and the Nation's security.

A. App-based security threats are more acute than ever before

Americans are constantly and increasingly on their phones.[4] Much of that time is spent on mobile apps.[5] Each app is a new opportunity for attackers. Our Nation's adversaries—China, Russia, North Korea, Iran, and others—know this and so have devoted substantial resources to targeting apps.[6] Because the injunction would prevent Google from adequately securing apps for Android users, sophisticated hackers can conceal malware in legitimate-looking apps, leaving unsuspecting users to click on an app that looks innocuous but enables access to their device or personal information.[7]

There are three primary methods of malware cyberattacks:

a. Traditional Malware: Spyware enables hackers to observe and extract data on a mobile device. For instance, last year, it was reported that Chinese hackers had

---

[4] Risa Gelles-Watnick, *American's Use Of Mobile Technology And Home Broadband*, PEW RSCH. CTR. (Jan. 31, 2024), https://perma.cc/27TZ-C2PX.

[5] *Mobile App Download Statistics And Usage Statistics (2025)*, BUILDFIRE, https://perma.cc/D9G2-QF56.

[6] *See generally* Office of the Director of National Intelligence, *Annual Threat Assessment Of The U.S. Intelligence Community* at 4 (Mar. 18, 2025), https://perma.cc/TS4U-V226.

[7] *See, e.g.*, Lily Hay Newman, *Hundreds Of Scam Apps Hit Over 10 Million Android Devices*, WIRED (Sept. 29, 2021), https://perma.cc/4R69-BRWA.

breached the cellphone of President Donald Trump's personal attorney, obtaining voice recordings and text messages.[8] And the U.S. government has become increasingly concerned that apps like TikTok could be used by China to inject malware onto Americans' phones en masse.[9] Malware can compromise sensitive or secure information on government employees' devices[10] (a threat based on both the content of the information and blackmail potential), infiltrate apps designed for the U.S. armed forces,[11] or surveil U.S. government officials' movements.[12] Malware can jeopardize critical physical infrastructure, including major sources of water, electricity, telecommunications, gas, and industrial plants.[13]

---

[8] Paula Reid et al., *Trump Attorney's Phone Tapped By Chinese Hackers, Sources Tell CNN*, CNN (Nov. 8, 2024), https://perma.cc/36H5-K824.

[9] James Andrew Lewis, *TikTok and National Security*, CSIS (Mar. 13, 2024), https://perma.cc/2L9E-R2V9.

[10] Ellen Nakashima & Tim Starks, *At Least 50 U.S. Government Employees Targeted With Phone Spyware Overseas*, WASH. POST (Mar. 27, 2023), https://tinyurl.com/wuw54wm4; Ben Schreckinger, *How Russia Targets The U.S. Military*, POLITICO (June 12, 2017), https://perma.cc/ZUV9-VHN7.

[11] Ellyne Phneah, *Military Mobile Apps Useful, But Security Threats Loom*, ZDNET (July 26, 2012), https://perma.cc/SVR8-PZD9.

[12] Byron Tau & Dustin Volz, *NSA Warns Cellphone Location Data Could Pose National-Security Threat*, WALL ST. J. (Aug. 4, 2020), https://perma.cc/4T4V-D7VW.

[13] Will Carless & Michael Loria, *Cyberattacks On Critical US Infrastructure Keep Happening. How Worried Should We Be?*, USA TODAY (Oct. 25, 2024), https://perma.cc/SKJ4-ZS8Z.

b. Ransomware: In a ransomware attack, an adversary freezes access to the user's files in exchange for a ransom. If not paid, the adversary may permanently delete the data. Ransomware's threat extends beyond just one user's data, because ransomware may be transferred to a networked system via a shared wireless connection. Ransomware attacks have targeted U.S. hospitals, an oil pipeline, and more.[14]

c. Man-in-the-Middle Intrusions: In a Man-in-the-Middle attack, an adversary positions itself "between two communicating parties in order to intercept and/or alter data traveling between them."[15] Usually, a phone's operating system will verify that apps have the proper certificates to authenticate their identity as a trusted entity.[16] But a malicious app can tamper with the phone's database of trusted entities and so subvert the verification process.

The national-security implications of these attacks are twofold. First, malware affecting individuals' data on enough devices for a large-scale attack has national

[14] Bree Fowler, *Ransomware Rises As A National Security Threat As Bigger Targets Fall*, C-NET (Oct. 18, 2021), https://perma.cc/X3ET-H5UQ; Barbara Booth, *The Government Is Getting Fed Up With Ransomware Payments Fueling Endless Cycle Of Cyberattacks*, CNBC (Oct. 18, 2024), https://perma.cc/TAL2-VXDX.

[15] Man-in-the-middle-attack (MitM), NAT'L INST. STANDARDS & TECH., https://perma.cc/K9UZ-WC6X.

[16] David Cooper et al., *RFC 5280, Internet X.509 Public Key Infrastructure Certificate And Certificate Revocation List (CRL) Profile* § 3.2 (May 2008).

consequences. Second, malware propagated to one device can be transmitted to others.

B. The injunction limits Google's ability to protect national security

Outside of litigation, the government has recognized that it cannot protect the Nation's cybersecurity alone. It must rely on the private sector to identify and neutralize cyber threats.[17] Google has long been an able partner in protecting Americans' cybersecurity. But the district court's injunction would hamstring its ability to do so by requiring Google to provide increased access to third-party app stores while limiting its ability to impose sufficient security screening and imposing a Technical Committee to review Google's security measures.

Because Android is not a walled garden, users can peruse the Google Play Store—which carries stringent security standards—or more than 400 third-party app stores. Some third-party app stores are "vectors for an elevated volume of pirated apps, malware, or inappropriate content."[18] Third-party app stores that lack the same stringent security processes as the Google Play Store can be especially potent vectors of malware.

---

[17] Statement of Christopher A. Wray, Director, FBI, Before the U.S. Senate Comm. on Homeland Sec. & Governmental Affs., "Threats to the Homeland" at 7 (Oct. 31, 2023), https://perma.cc/KSS3-83S9.

[18] Dkt. 981-3 ¶ 71 (Cunningham).

Examples of these types of attacks abound, and more threats arise every day. For instance, Meta recently announced that more than 400 apps on Android and iOS were seemingly mundane photo editing or gaming apps but obtained users' Facebook login information for nefarious purposes.[19] Just a few months ago, it was reported that a North Korean hacking group had placed on the Google Play Store so-called "KoSpy" apps, which were utility apps that surreptitiously collected users' data, including text messages and screenshots.[20] And just last month, Iranian-affiliated hackers were found to have used spyware disguised as VPN and banking apps to seize users' data.[21]

These attacks can also be specifically targeted at military personnel, undermining national security even more directly. For example, Hamas operatives created an app store that was targeted to Israeli soldiers and had a number of seemingly innocuous apps, including a chat app.[22] When downloaded, the chat app gave Hamas operatives almost entire control over the user's phone and data.[23]

---

[19] Michael Kan, *Meta Uncovers 400 Malicious Android, iOS Apps Designed To Steal Logins*, PC MAG (Oct. 7, 2022), https://perma.cc/2RB9-9A9D.

[20] Michael Kan, *Suspected North Korean Hackers Infiltrate Google Play With 'KoSpy' Spyware*, PC MAG (Mar. 12, 2025), https://perma.cc/TJK5-BG63.

[21] *Lookout Discovers Iranian APT MuddyWater Leveraging DCHSpy During Israel-Iran Conflict*, LOOKOUT (July 21, 2025), https://perma.cc/7DHN-FP63.

[22] Netanel Flamer, THE HAMAS INTELLIGENCE WAR AGAINST ISRAEL 84-90 (2024).

[23] *Id.*

Although well-capitalized companies with years of experience managing cybersecurity risks, like Apple and Google, can quickly identify and remove these apps (as Google promptly did with the KoSpy apps), smaller third-party app stores may not be willing or able to do so. For example, one app that was publicly reported to be malicious in November 2022 remained available in a prominent third-party app store in June 2024.[24] That is why numerous government agencies uniformly caution against the use of third-party app stores.[25]

The injunction would immediately undermine users' security by transferring the security burden from Google to the user, who is inherently less equipped to detect and evade sophisticated malware traps set by experienced malicious actors.

First, requiring Google to allow developers to provide links directly to users would create inherent security risks, since Google does not have the capability to monitor linked websites for security, and users would be left to trust app developers of varying sophistication.[26] Doing so also hinders the ability to identify and respond

[24] Dkt. 981-3 ¶ 73.

[25] National Security Agency, *Mobile Device Best Practices* at 2 (Oct. 2020), https://perma.cc/VWM2-PYAD; *see also Government Experts In The U.S.: Don't Sideload*, TRUSTED FUTURE, https://perma.cc/UHY5-M22G (compiling reports from the NSA, FTC, SBA, GSA, DHS, CISA, FBI, and NIST emphasizing reliance on "trusted" sources like Google, and recommending against sideloading and downloading from third-party app stores).

[26] Dkt. 1020-3 ¶ 6 (Kleidermacher).

to threats because Google would lose visibility into activity at the app level, hindering integrated cybersecurity risk management.

Second, requiring Google to distribute third-party app stores would increase the risk of similar security threats.[27] In an illustrative example, a cyberhacking group flooded the Google Play Store, and other app stores, with seemingly harmless apps such as translators and calculators, which turned out to be malicious.[28] While Google quickly identified and removed the offending apps, many remained available on third-party app stores.[29] Under the injunction, Google could well be required to distribute app stores containing the very same apps it banned from its platform. Alternatively, Google would have to create a product to review every single app uploaded onto every single third-party app store, which Google conservatively estimates would take a year to build.[30] And rushing an essential security product to market could have catastrophic consequences.

Third, requiring Google to allow third-party app stores access to the Google Play Store would allow malicious actors to set up third-party app stores populated with the Google Play Store library of apps, providing a veneer of legitimacy. But a

---

[27] *See* Dkt. 1017 ¶ 12.

[28] Newman, *supra*.

[29] *Id.*

[30] Dkt. 981-5 ¶ 22 (Kleidermacher). The injunction contemplates Google creating this product within eight months. *See* Dkt. 1017 ¶ 12.

malicious actor can then easily "clone" those apps with realistic-seeming thumbnails linked to malicious code instead of trusted Google Play Store apps.[31] A mere warning that a user is leaving the Google Play Store platform—on the way to a third-party app store designed to look like the Google Play Store—does not nearly address the severity and sophistication of the possible threats.

Finally, the Technical Committee cannot adequately safeguard users from these threats because of its purpose and structure. The Committee exists to monitor whether Google's measures threaten competition—not to ensure that the Google Play Store and third-party app stores are safe for the millions who use them. And Epic Games has influence over appointing two of the of the three people who will comprise the Committee—Epic Games and Google can each select one Committee member and the third member is selected by the other two. That gives a sole app developer an outsized influence to determine cybersecurity requirements for hundreds of thousands of app developers. There is no guarantee that Epic Games will appoint members with the appropriate technical expertise and qualifications to maintain users' security.

There are also no requirements for how active the Committee must be, how long it may take to make decisions about whether Google's measures are appropriate, and so on. If the Committee dawdles, or if disputes must go to the

[31] Dkt. 1020-3 ¶ 16 (Kleidermacher); *see also* Dkt. 1020-3, Ex. A.

district court, security threats will proliferate in the meantime. That is why the Supreme Court cautioned against judicial antitrust remedies that require "day-to-day controls." *Trinko*, 540 U.S. at 415. Indeed, even the district court recognized that "[t]here is a complicated world of security that, as a district judge, I should not be involved in."[32]

But the injunction would place the district court and Technical Committee at the center of managing security for millions. Even one misstep could have disastrous consequences for individuals' and the Nation's cybersecurity.

CONCLUSION

The Court should grant rehearing.

[32] Dkt. 977, May 23, 2024 Hearing Tr. at 82:2-3. Though the panel identified other arrangements it contends involve a level of specialized expertise similar to that required of the Technical Committee, those examples are inapposite. Op. 58-59. None involves the creation of what is essentially a regulatory body to govern an area as complex, dynamic, and fraught as real-time cybersecurity for an ecosystem touching millions of users where a coordinated, immediate response to active threats is critical. Indeed, the risk of this task is extraordinary and without precedent.

Dated: August 25, 2025

Respectfully submitted,
/s/ Roy T. Englert, Jr.

Roy T. Englert, Jr.
Ariel N. Lavinbuk
Shikha Garg
HERBERT SMITH FREEHILLS
KRAMER (US) LLP
2000 K Street NW, 4th Floor
Washington, DC 20006
(202) 775-4500
roy.englert@hsfkramer.com
ariel.lavinbuk@hsfkramer.com
shikha.garg@hsfkramer.com

Counsel for Amici Curiae

APPENDIX: List of *Amici Curiae*

Paul Lekas served as Deputy General Counsel (Legal Counsel) at the Department of Defense, Director of Research and Analysis and Senior Legal and Strategy Advisor at the National Security Commission on Artificial Intelligence, and General Counsel at the National Commission on Military, National, and Public Service.

Lieutenant General (Ret.) Joseph Anderson, United States Army, served as Deputy Chief of Staff of the Army for Operations, Plans, and Training.

Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor Emeritus of Computer Science at Columbia University, a former affiliate law professor at Columbia Law School, and currently a Senior Affiliate Scholar at the Georgetown University Institute for Technology Law & Policy. He is also the former Chief Technologist at the Federal Trade Commission.

Tatyana Bolton leads the cybersecurity practice at Monument Advocacy. She has also served as the Managing Senior Fellow at the R St Institute for Cybersecurity and National Security and the cyber policy lead at the Cybersecurity and Infrastructure Security Agency.

Joel Brenner is a Senior Research Fellow at the MIT Center for International Studies. He has also served as Inspector General and Senior Counsel at the National Security Agency and as head of counterintelligence at the Office of the Director of National Intelligence.

Lieutenant General (Ret.) John (Jack) N.T. Shanahan, United States Air Force, served as the inaugural Director of the Department of Defense Joint Artificial Intelligence Center.

David R. Shedd served as Director (Acting) and Deputy Director for the Defense Intelligence Agency and as Special Assistant to the President and Senior Director for Intelligence Programs and Reform on the National Security Council.

Gene Tsudik is a Distinguished Professor of Computer Science at the University of California, Irvine.

CERTIFICATE OF COMPLIANCE

1. This brief complies with the applicable type-volume and length limitations because it contains 2,855 words, excluding the items exempted by Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface and typestyle requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared in a proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman font.

Dated: August 25, 2025

/s/ Roy T. Englert, Jr.
Roy T. Englert, Jr.