

No. 25-521

---

IN THE  
**Supreme Court of the United States**

---

GOOGLE LLC, *et al.*,  
*Petitioners,*

v.

EPIC GAMES, INC.,  
*Respondent.*

---

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

---

BRIEF OF COMPUTER SECURITY EXPERTS  
JOHN MITCHELL, SERGE EGELMAN, KEVIN  
BUTLER, AMIT ELAZARI, GUOFEI GU, AND  
SHARAD MEHROTRA AS *AMICI CURIAE*  
SUPPORTING PETITIONERS

---

ROBERT T. SMITH  
*Counsel of Record*  
NEAL S. MEHROTRA  
KATTEN MUCHIN ROSENMAN LLP  
1919 Pennsylvania Avenue, N.W.  
Suite 800  
Washington, DC 20006  
robert.smith1@katten.com  
202-625-3500

*Counsel for Amici Curiae*

---

**Table of Contents**

Table of Authorities..... ii

Interests of *Amici Curiae* .....1

Summary of the Argument .....4

Argument.....8

I. The injunctive relief the district court awarded to Epic Games raises unprecedented security issues for over one hundred million Android users.....8

    A. The injunction will lead to a proliferation of malicious weblinks, exposing millions of users of Google’s Play Store to extensive security risks ..... 11

    B. The injunction will lead to an explosion of scam app stores and weaken Android’s security ecosystem worldwide ..... 14

II. No court has considered the risks and benefits of the remedies the district court ordered here, escalating the need for review by this Court..... 19

Conclusion .....26

## Table of Authorities

### CASES:

<i>Granny Goose Foods, Inc. v. Bhd. of Teamsters &amp; Auto Truck Drivers Loc. No. 70</i> , 415 U.S. 423 (1974) .....	7, 21
<i>La Quinta Worldwide LLC v. Q.R.T.M. S.A. DE C.V.</i> , 762 F.3d 867 (9th Cir. 2014) .....	21
<i>Mayo v. Lakeland Highlands Canning Co.</i> , 309 U.S. 310 (1940) .....	7, 20-22
<i>Purcell v. Gonzales</i> , 549 U.S. 1 (2006) .....	21-22
<i>Trump v. Int’l Refugee Assistance Project</i> , 582 U.S. 571 (2017) .....	20
<i>United States v. Merz</i> , 376 U.S. 192 (1964) .....	22

### STATUTES:

28 U.S.C. § 455 .....	23
-----------------------	----

### RULES:

Fed. R. Civ. P. 52(a)(1) .....	7, 21
Fed. R. Civ. P. 52(a)(2) .....	21
Fed. R. Civ. P. 53(a)(2) .....	23
Fed. R. Civ. P. 65(d)(1) .....	7, 21

## OTHER AUTHORITIES:

Admin. Office of the U.S. Courts, <i>Electronic Filing Scam Targets Attorneys</i> (Nov. 6, 2024).....	5
Admin. Office of the U.S. Courts, <i>Information Systems and Cybersecurity – Annual Report 2022</i> .....	13
Bitdefender, <i>Unveiling Mobile App Secrets: A 6-Month Deep Dive into Surprising Behavior Patterns</i> , Jan. 8, 2024 .....	11, 15
Eduardo Blázquez, <i>et al.</i> , <i>Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem</i> , 2021 IEEE Symposium on Security and Privacy 1606 (2021) .....	8, 16
Epic Games Store, <i>Browse</i> .....	25-26
Federal Bureau of Investigation, <i>On the Internet: Be Cautious When Connected</i> .....	13-14
Federal Bureau of Investigation, <i>Sextortion</i> .....	19
Federal Bureau of Investigation, <i>Spoofing and Phishing</i> .....	11-12
Cassidy Gibson, <i>et al.</i> , <i>Analyzing the Monetization Ecosystem of Stalkerware</i> , 2022 Proceedings on Privacy Enhancing Technology Symposium 105 (2024 Issue 4) .....	18
Global Anti-Scam Alliance, <i>Global State of Scams – 2023</i> .....	13
Google, <i>Device and network abuse</i> .....	11

Julie Jargon, <i>'Sextortion' Scams Involving Apple Messages Ended in Tragedy for These Boys</i> , Wall St. J., June 7, 2025.....	19
Platon Kotzias, <i>et al.</i> , <i>How Did That Get In My Phone? Unwanted App Distribution on Android Devices</i> , 2021 IEEE Symposium on Security and Privacy 53 (2021) .....	9-10, 12-13
Arthur R. Miller, <i>et al.</i> , 9C Federal Practice and Procedure (3d ed. 2025) .....	21-22
Nikita Samarin, <i>et al.</i> , <i>The Medium is the Message: How Secure Messaging Apps Leak Sensitive Data to Push Notification Services</i> , 2024 Proceedings on Privacy Enhancing Technology Symposium 967 (2024 Issue 1) .....	16, 18-19
Silviu Stahie, <i>Google Blocked More than 2 Million Apps from Being Published in Google Play</i> , Bitdefender, May 2, 2024 .....	17
Byron Tau, <i>Apple and Google to Stop X-Mode From Collecting Location Data From Users' Phones</i> , Wall St. J., Dec. 9, 2020 .....	17
U.S. Dist. Ct., N.D. Cal., <i>Beware of Fake Court E-mails</i> .....	5
The Verge, <i>Uber tried to fool Apple and got caught</i> , Apr. 23, 2017 .....	24

## Interests of *Amici Curiae*\*

*Amici curiae* are computer security experts—current and former academics who have studied and researched in the areas of computer security and privacy, and who have extensive experience analyzing the security and privacy risks of mobile applications. They have a substantial interest in ensuring that courts make informed, rational decisions about data security and privacy.\*\*

John Mitchell is the Mary and Gordon Crary Family Professor, professor of computer science, and by courtesy professor of electrical engineering and professor of education at Stanford University. He was previously chair of the Computer Science Department. Professor Mitchell's research focuses on programming languages, computer security and privacy, blockchain, machine learning, and technology for education. With over 250 publications and over 30,000 citations, he has led research projects on a range of topics, been a consultant or advisor to many companies, and served as editor-in-chief of the *Journal of Computer Security*.

---

\* Counsel for *amici curiae* provided notice to the counsel of record for all parties more than ten days before the filing of this brief. No counsel for any party authored this brief in whole or in part. No person or entity—other than *amici* or their counsel—made a monetary contribution specifically for the preparation or submission of this brief.

\*\* Although *amici* are affiliated with various academic and business institutions, they lend their support to this brief in their individual capacities only. Nothing in this brief should be construed as the position of the academic institutions and businesses with which they are affiliated.

Serge Egelman is the Research Director of the Usable Security and Privacy group at the International Computer Science Institute, which is an independent research institute affiliated with the University of California, Berkeley. He also holds a position as a research scientist within the Electrical Engineering and Computer Sciences Department at the University of California, Berkeley. He is a co-founder and Chief Scientist of AppCensus, Inc., which builds tools to test the privacy behaviors of mobile applications. He received his Ph.D. from Carnegie Mellon University's School of Computer Science; his research has been cited over 14,000 times; and he has testified before Congress on issues relating to the privacy and security of mobile applications.

Kevin Butler is the director of the Florida Institute for Cybersecurity and a professor of computer and information science and engineering at the University of Florida. Professor Butler's research focuses on the security of computers—from embedded and mobile devices to cloud computing systems—and the data they generate. He has led a research team that uncovered smartphone vulnerabilities that would allow hackers to take control of phones and extract private information without user knowledge. In response to his groundbreaking findings, LG and Samsung promptly developed a security patch. Professor Butler is a Senior Member of the Association of Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE), and he serves on the Computing Research Association Computing Community Consortium as an expert in computer security and privacy. According to Google Scholar, his work has been cited over 6,000 times, and he has received the

National Science Foundation's prestigious CAREER Award. He received his Ph.D. in Computer Science and Engineering from the Pennsylvania State University.

Amit Elazari is a co-founder and the chief executive officer of OpenPolicy, the world's first tech-enabled policy intelligence and engagement platform, which aims to democratize access to policy to entities of all sizes. Dr. Elazari teaches at the School of Information and Cybersecurity at the University of California, Berkeley, and at Reichman University, and serves as a member of the External Advisory Committee for the UC Berkeley Center of Long-Term Cybersecurity. Prior to OpenPolicy, she was Head of Global Cybersecurity Policy at Intel Corporation, responsible for shaping and executing Intel's global security policy and government affairs engagement across all of Intel Technologies. She holds a Doctoral Degree in the Law (J.S.D.) from the University of California Berkeley School of Law.

Guofei Gu is a professor, the holder of the Eppright Professorship in Engineering, and the Director of the Secure Communication and Computer Systems (SUCCESS) Lab in the Department of Computer Science and Engineering at Texas A&M University. His research interests are in network and systems security, including software-defined programmable security, malware and intrusion detection, Artificial Intelligence security, and security related to mobile devices. Professor Gu is also an IEEE Fellow and an ACM Distinguished Member. According to Google Scholar, his work has been cited over 20,000 times. He received his Ph.D. in Computer Science from the

College of Computing at the Georgia Institute of Technology.

Sharad Mehrotra is a Distinguished Professor of Computer Science at the University of California, Irvine. He is a fellow of ACM and of IEEE. Professor Mehrotra's research expertise spans database management, distributed systems, and secure databases, including computer and cloud security, data privacy, cryptography, software engineering, and machine learning. He has received numerous awards and honors, including the 2011 SIGMOD Best Paper Award, the 2007 DASFAA Best Paper Award, DASFAA ten-year best paper award for 2013, the 1998 CAREER Award from the National Science Foundation, ACM ICMR Best Paper Award for 2013, IEEE SRDS Best paper award 2018, IEEE NCA best paper award 2019, and IEEE Percom 2022 Best Paper Award. His over 500 articles have been cited over 28,000 times according to Google Scholar. His pioneering contributions to the field include his work on encrypted search on database as a service that was recognized through the prestigious SIGMOD Test of Time award in 2012 and DASFAA ten-year best paper award in 2014. Prior to entering academia, Professor Mehrotra was a Scientist at Panasonic Technologies. He received his Ph.D. from the University of Texas at Austin in Computer Science.

### **Summary of the Argument**

The Internet can be a scary place—take the federal judiciary's recent experience. Lawyers and parties who had signed up for electronic filing notifications started receiving seemingly legitimate e-mail notifications with a link to access case documents on court

websites. As it turned out, scammers were behind the e-mails; the websites they were directing people to were malicious; and some people were unwittingly surrendering sensitive personal information and installing malware on their computers. *See* Admin. Office of the U.S. Courts, *Electronic Filing Scam Targets Attorneys* (Nov. 6, 2024).<sup>1</sup>

To avoid being a victim of the scam, the federal judiciary advised users to “[n]ever download attachments or click on links from unofficial or questionable sources.” *Id.* And users were instructed to validate e-mails and “case documentation directly through [their] local federal court’s CM/ECF system.” *Id.*; *see also* U.S. Dist. Ct., N.D. Cal., *Beware of Fake Court E-mails* (providing similar advice).<sup>2</sup>

The Administrative Office of the United States Courts drew upon two sound practices when it comes to computer and information security. First, downloading questionable attachments or clicking on unverified links can present a serious security risk. Second, where there is a legitimate, centralized repository of information, users can use that source to verify that a specific communication is not a scam.

In this case, however, the district court issued a permanent injunction that violates these principles as applied to the more than one hundred million users whose devices run on Google’s Android operating system. First, Google was ordered to permit app

---

<sup>1</sup> <https://www.uscourts.gov/news/2024/11/06/electronic-filing-scam-targets-attorneys>.

<sup>2</sup> <https://www.cand.uscourts.gov/notices/beware-of-fake-court-emails/>.

developers to include external weblinks (known as linkouts) in apps available for download on Google's Play Store—links that send users to unknown and potentially untrustworthy websites. Second, the injunction mandates that Google provide the Play Store's full catalog of two-million-plus apps to anyone who wishes to run a rival app store, and it compels Google to list on the Play Store the third-party-app-store app of these third-party app stores. These provisions will lead to an explosion of external weblinks displayed within apps downloaded on Google's Play Store or through Play Store listings, increasing the likelihood that users will be directed to websites where they might inadvertently install malware onto their devices or surrender highly sensitive personal and financial information. And the injunction will lead to the proliferation of scam app stores, which will increase the prevalence of pirated and malicious apps on Android devices and impair the ability of users to verify the legitimacy of the apps that they might wish to download.

Remarkably, no court—neither the district court nor the Court of Appeals for the Ninth Circuit—has considered the risks and benefits of the remedies the district court awarded here. That screams out for this Court's intervention.

When it came to the security interests of over one hundred million Android users, the district court threw up its hands:

As Google has suggested, there are potential security and technical risks involved in making third-party apps available, including rival app

stores. *The Court is in no position to anticipate what those might be, or how to solve them.*

App.89a (emphasis added). Punting, the court left some of these issues to a technical committee to sort out on the backend. *Id.* And even then, there are critical gaps in this process that make it impossible for Google to fully mitigate the risks presented by the injunction.

Compounding these errors, the Ninth Circuit blessed the district court's award of unprecedented injunctive relief, not on the strength of any "findings" on how the injunction would affect the security interests of tens of millions of non-parties, but instead by mere dint of the fact that the district court had before it a "robust record." App.63a. That contravened this Court's precedents and the Federal Rules of Civil Procedure.

As this Court has recognized, when it comes to the equities of an injunction, district courts are required to make "findings of fact upon these vital issues"—not leave those tasks to someone else. *Mayo v. Lakeland Highlands Canning Co.*, 309 U.S. 310, 316 (1940). Rules 52(a)(1) and 65(d)(1) of the Federal Rules of Civil Procedure demand no less. And the remedy in this situation is equally clear—"where the required findings of fact and conclusions of law have not been set forth, the order is invalid." *Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck Drivers Loc. No. 70*, 415 U.S. 423, 443 n.17 (1974) (explaining the requirement of vacatur in the context of a preliminary injunction).

This Court’s review is therefore urgently needed—to protect one hundred million Android users from unprecedented security risks, and to emphasize the importance of judicial factfinding before federal courts award injunctive relief, particularly at the scope and scale awarded here.

### Argument

#### **I. The injunctive relief the district court awarded to Epic Games raises unprecedented security issues for over one hundred million Android users.**

Google’s Android software is “the most used operating system ever”—more than Microsoft Windows or Apple Mac OS. Eduardo Blázquez, *et al.*, *Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem*, 2021 IEEE Symposium on Security and Privacy 1606, 1606 (2021).<sup>3</sup> Worldwide, over 2.5 billion devices—from smartphones to tablets and even some computers—are running on Android daily. *Id.*

Among its many virtues, Android’s system is open. Unlike Apple, which forces its users to use Apple’s App Store to download apps on Apple devices, Google does not force Android users to download and install apps using the Play Store, Google’s online store for downloading Android apps. To the contrary, Android users may also download apps from third-party app stores or websites—referred to as sideloading. And unlike Apple, which is the exclusive manufacturer of devices that run Apple’s iOS operating system

---

<sup>3</sup> <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&ar-number=9519485>.

(namely, iPhones and iPads), Google allows other manufacturers to produce devices that run Android. The result is a robust marketplace for both Android apps and the devices that run those apps.

Although Android’s openness should be heralded for providing choice to consumers, promoting competition, and forcing Apple to make enhancements to its own offerings, this openness creates unique security challenges that Google has attempted to mitigate within one of the ecosystems that it controls: Google’s Play Store. Google’s approach to the Play Store is multifaceted, but two aspects warrant further explanation here. First, Google makes developers who wish to make their apps available on the Play Store adhere to a variety of security parameters, which include forbidding developers from including linkouts in apps available on the Play Store—linkouts that could misdirect users to malicious and unwanted websites. Second, Google invests substantial resources to prevent problematic apps from appearing in Google’s Play Store in the first place; it removes apps when further investigation reveals that they are malicious or subject to security vulnerabilities; and it helps implement millions of updates each year to improve the quality of apps available on Android devices.

Outside the Play Store and a handful of well-run third-party app stores like Amazon’s Appstore and Samsung’s Galaxy Store, it’s the Wild West. One study found that, globally, alternative markets are “on average five times riskier (3.2% VDR) than the Play market (0.6%).” Platon Kotzias, *et al.*, *How Did That Get In My Phone? Unwanted App Distribution on Android Devices*, 2021 IEEE Symposium on Security

and Privacy 53, 54 (2021).<sup>4</sup> Some stores, like Amazon’s, “are almost as safe as the Play market, but users of other top alternative markets have up to 19 times higher probability of encountering an unwanted app.” *Id.* And that just focuses on third-party app stores. Downloads directly from the web are currently rare “but have significantly higher risk (3.8% VDR) than downloads from markets, even alternative ones (3.2%).” *Id.*

In this case, however, the district court awarded a single private party, Epic Games, sweeping injunctive relief that will weaken the security of Google’s app ecosystem in two significant ways, adversely affecting more than one hundred million users based in the United States and others worldwide. *First*, it ordered Google to allow linkouts within apps and listings available on Google’s Play Store. *Second*, it mandated that Google provide the Play Store’s full catalog of apps—more than two million of them—to anyone who wishes to run a rival app store, and it compelled Google to list on the Play Store the third-party-app-store apps of rival third-party app stores. As explained below, the benefits of these provisions to Epic are not obvious, let alone to consumers at large, and the harms to the security of Android users are drastic and cannot reasonably be limited through risk-mitigation strategies.

The Court should grant Google’s petition to address the critical security flaws in the district court’s injunction order.

---

<sup>4</sup> <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&ar-number=9519429>.

**A. The injunction will lead to a proliferation of malicious weblinks, exposing millions of users of Google’s Play Store to extensive security risks.**

Under paragraph 10 of the injunction, Google may not prohibit developers from embedding within the apps they distribute through the Play Store external links to download apps outside the Play Store. *See* App.69a. This is a recipe for disaster.

Google prohibits developers from including external links in any app the developer distributes through the Play Store because such links pose a serious security risk. *See* Google, *Device and network abuse*.<sup>5</sup> Links can direct users to anywhere on the Internet.

As the federal judiciary knows all too well, if links direct users to sites that are malicious but appear legitimate, they could lead to a variety of security risks. On Android devices, that could include tricking users into installing malware, directing users to provide sensitive financial and personal information, stealing users’ data, tracking users’ activities on the Internet, and even accessing a device’s location, text messages, microphone, and camera. *See* Bitdefender, *Unveiling Mobile App Secrets: A 6-Month Deep Dive into Surprising Behavior Patterns*, Jan. 8, 2024<sup>6</sup>; *see also* Federal Bureau of Investigation, *Spoofing and Phishing* (describing the process by which cybercriminals can use

---

<sup>5</sup> <https://support.google.com/googleplay/android-developer/answer/16273414?hl=en&sjid=11373020642207796491-NA#>.

<sup>6</sup> <https://www.bitdefender.com/en-us/blog/labs/unveiling-mobile-app-secrets-a-6-month-deep-dive-into-surprising-behavior-patterns/>.

links to cause users to “download malicious software, send money, or disclose personal, financial, or other sensitive information”).<sup>7</sup>

The dangers of the district court’s injunction are particularly significant because users would encounter these links in a previously trusted environment. Because Google has spent years cultivating a secure user experience within the Play Store and apps available on Play, users will be more prone to trust these links, exposing them to all the risks outlined above. *See, e.g., How Did That Get In My Phone?, supra*, at 61. And whereas Google can vet the apps that it makes available through the Play Store, mitigating the risk of malware and quickly removing malicious and unwanted apps from the Play Store and users’ devices through centralized mechanisms, Google cannot possibly track every app available for download on the Internet that would be accessible through the kinds of linkouts mandated by the district court.

As noted, Google does not force Android users to download apps through Google’s Play Store; they are free to download apps from external sources, including from third-party app stores. But for those users who elect to use Google’s Play Store, many prefer Play’s security features. Academic research suggests that, outside of Google Play and a handful of other well-run app stores, users of other top alternative markets are substantially more likely to encounter malicious apps, and the risks posed by web-downloads are

---

<sup>7</sup> <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing>.

significantly higher still. *How Did That Get In My Phone?*, *supra*, at 54.

Cybercriminal organizations, state-sponsored actors, and freelancers are already highly successful at tricking people over insecure forms of communication, including e-mails, text messages, and telephone calls. According to one study, 78 percent of mobile users experienced at least one scam in a given year, and those scams are usually initiated by sending links to get users to install malicious applications. Global Anti-Scam Alliance, *Global State of Scams – 2023*, at 12-13.<sup>8</sup>

Moreover, these risks are not limited to an individual user’s Android device; they could expose business and governmental networks to illicit attacks. Among other things, cybercriminals could gain access to passwords and other sensitive information that Android users also use to access their work accounts. That, in turn, could expose State secrets and third-party intellectual property to theft or destruction. Likely for these reasons, the Administrative Office of the United States Courts recognizes the “threat” posed to its networks by court personnel accessing “malicious websites.” Admin. Office of the U.S. Courts, *Information Systems and Cybersecurity – Annual Report 2022*<sup>9</sup>; see also Federal Bureau of Investigation, *On the Internet: Be Cautious When Connected* (warning Internet users

---

<sup>8</sup> <https://www.scribd.com/document/679758338/Global-State-of-Scams-Report-2023-Global-GASA-final>.

<sup>9</sup> <https://www.uscourts.gov/statistics-reports/information-systems-and-cybersecurity-annual-report-2022>.

not to access unverified links that could steer users to spoofed websites).<sup>10</sup>

Allowing malicious actors to communicate through linkouts embedded in apps available for download on Google's Play Store will only exacerbate these problems, reducing those few regions of the Internet that users can generally trust.

**B. The injunction will lead to an explosion of scam app stores and weaken Android's security ecosystem worldwide.**

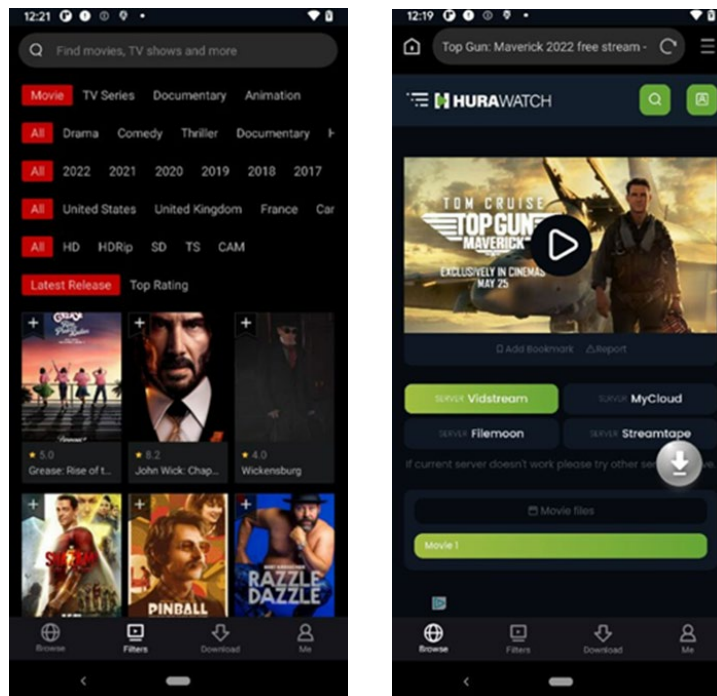
Under paragraphs 11 and 12 of the injunction, Google must distribute competitor app stores through its Play Store and provide those competitors with access to Play's entire catalog of apps. App.69a-70a. These paragraphs present a host of problems that threaten to weaken Android's app ecosystem worldwide.

To start, paragraphs 11 and 12 will lead to the proliferation of scam and substandard app stores that can rely upon Google's backend work to hawk their wares. An app store requires investment and technical know-how to attract users and gain legitimacy. But under the injunction, Google must provide its full catalog of apps to any applicant who requests access, App.69a-70a, meaning anyone can quickly populate an app store with over 2 million apps. Through this mechanism, the injunction makes it too easy for malicious and shoddy app stores to feign legitimacy.

---

<sup>10</sup> <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/on-the-internet>.

The risks associated with scam and substandard app stores are already very real, and the district court’s injunction threatens to make the problem worse. Scam app stores lure users by appearing legitimate, but they can fake and clone apps that wreak havoc on unsuspecting users. For example, one app disguised itself as a movie streaming service:



Bitdefender, *supra*, n.6. This app was actually malware that “can access contacts data, calendar data, sensor data, send and receive [text messages], read and write on external storage, access the device[’s] location, read or write [telephone] call logs or even redirect [calls] to a different number, initiate or answer phone call[s], record audio [using the device’s microphone], recognize physical activity [from the device’s proximity and other sensors],” and “access the

camera” on the device. *Id.* Although this app was removed by Google from the Play Store, it is “still likely available to download from other sources.” *Id.*

Criminals already target unsuspecting users by cloning popular apps like Netflix, Instagram, Spotify, and others to pry users of their passwords, infect their devices with malware, and obtain access to sensitive personal and financial information, *id.*—an unfortunate practice that occurs within the Android ecosystem. Paragraphs 11 and 12 would hand cybercriminals the tools needed to make more effective storefronts for listing such reverse-engineered apps.

Even benevolent but substandard app stores pose security and safety risks for consumers. Operating systems and apps require frequent updates to ensure that they run properly and to eliminate security and safety vulnerabilities. *See, e.g.,* Nikita Samarin, *et al.*, *The Medium is the Message: How Secure Messaging Apps Leak Sensitive Data to Push Notification Services*, 2024 Proceedings on Privacy Enhancing Technology Symposium 967, 967 (2024 Issue 1).<sup>11</sup> Yet research has “demonstrated that many software privacy issues”—for example, “the inappropriate disclosure of sensitive user information”—occur because developers, like all humans, make mistakes. *Id.* Substandard stores—the kinds propped up by the district court’s injunction—risk disseminating out-of-date apps with critical security deficiencies and not updating them on a timely basis. *See Trouble Over-The-Air, supra*, at 1606.

---

<sup>11</sup> <https://petsymposium.org/popets/2024/popets-2024-0151.pdf>.

In contrast, well-run app stores improve the supply chain of apps by investing in the resources and technical know-how necessary to help block and remove malicious apps from the top down, benefitting millions upon millions of users quickly and efficiently. In 2023 alone, “Google stopped 2.28 million policy-violating apps from being published on Google Play,” and it blocked 333,000 bad accounts for confirmed security violations. Silviu Stahie, *Google Blocked More than 2 Million Apps from Being Published in Google Play*, Bitdefender, May 2, 2024.<sup>12</sup>

There are numerous examples where well-run app stores have removed dangerous apps. For example, a company known as X-Mode had secretly embedded location-tracking software in a variety of apps, and the company then sold data of Americans’ movements—which could include seeking care at medical providers or attending political events. Soon after this scheme was revealed, Google and Apple were successful in removing X-Mode’s tracking software from any application present in their app stores. *See, e.g., Byron Tau, Apple and Google to Stop X-Mode From Collecting Location Data From Users’ Phones*, Wall St. J., Dec. 9, 2020.<sup>13</sup> That kind of coordinated action is simply not available at fly-by-night app stores.

As another example, Google took actions to ban from the Play Store “stalkerware” apps, which

---

<sup>12</sup> <https://www.bitdefender.com/en-us/blog/hotforsecurity/google-blocked-more-than-2-million-apps-from-being-published-in-google-play>.

<sup>13</sup> <https://www.wsj.com/articles/apple-and-google-to-stop-x-mode-from-collecting-location-data-from-users-phones-11607549061>.

covertly track the location of targets who have unknowingly had such apps installed on their phones, leading to a significant reduction of available stalkerware on Android devices. Cassidy Gibson, *et al.*, *Analyzing the Monetization Ecosystem of Stalkerware*, 2022 Proceedings on Privacy Enhancing Technology Symposium 105, 119 (2024 Issue 4).<sup>14</sup> Meanwhile, outside the Play Store, many new stalkerware apps have been discovered. *Id.* This example shows how Google has improved the electronic and physical safety of mobile-app users in a manner that has proven ineffective outside of well-run app stores.

The need for well-run apps stores is even more critical because of the virtues and vices of democratized app development. As the authors of one article noted, the Internet has allowed anyone to “become a software engineer and distribute software worldwide,” which is by and large “a good thing,” but it also “raises issues of professional responsibility that have long been addressed by other more mature branches of engineering.” *The Medium is the Message, supra*, at 977. “In most jurisdictions, one cannot simply decide to become a civil engineer and erect a multistory building.” *Id.* Plans are checked against building codes; the building is inspected at various stages of construction; and even after it is complete, the building can be condemned if it is no longer safe for habitation. *Id.* Outside of well-run app stores, no comparable entities operate in the space of computer software.

The stakes here are alarmingly high. Malicious and poorly developed apps may “pose risks to user

---

<sup>14</sup> <https://petsymposium.org/popets/2022/popets-2022-0101.pdf>.

safety—even lethal ones.” *Id.* For example, “online messaging apps are increasingly used by activists living in oppressive regimes, who may find themselves in serious jeopardy if their communications are inappropriately revealed.” *Id.* (internal footnote omitted). Closer to home, there has been a troubling surgency of “sextortion” whereby criminals have pried young users of sensitive photographs and other information and targeted them for blackmail—leaving many young Americans so distraught they have taken their own lives as a direct result of the stress this has inflicted. *E.g.*, Federal Bureau of Investigation, *Sextortion*<sup>15</sup>; Julie Jargon, ‘Sextortion’ Scams Involving Apple Messages Ended in Tragedy for These Boys, *Wall St. J.*, June 7, 2025.<sup>16</sup>

The district court’s injunction would make it too easy for people to set up app stores who, quite frankly, have no business doing so. And the results are predictable: The Android ecosystem will become significantly less safe and secure for users worldwide if the district court’s injunction is implemented.

**II. No court has considered the risks and benefits of the remedies the district court ordered here, escalating the need for review by this Court.**

Beyond the critical importance of the issues raised in Google’s petition as it relates to the security and safety of millions of non-parties, there are critical

---

<sup>15</sup> <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion>.

<sup>16</sup> [https://www.wsj.com/tech/personal-tech/sextortion-scam-teens-apple-icmessage-app-159e82a8?gaa\\_at](https://www.wsj.com/tech/personal-tech/sextortion-scam-teens-apple-icmessage-app-159e82a8?gaa_at).

deficiencies of process that heighten this Court’s need to intervene. Most notably, the district court should have made factual findings related to the equities and then drew conclusions balancing the jury’s findings of alleged anticompetitive conduct, Epic’s claimed need for the various remedies that were on the table, and the potential benefits and harms associated with each of those remedies—particularly to the consuming public. But that never happened here.

Despite ample record evidence of the security risks discussed in this brief, the district court made no findings about those risks, let alone weighed them against the perceived benefits of the remedies the district court ultimately awarded. It just gave up, confessing it was in “no position to anticipate what those [risks] might be, or how to solve them.” App.89a. Instead, it purported to leave these issues to a technical committee. *Id.*

Precedent and rule required more. Crafting an “injunction is an exercise of discretion and judgment, often dependent as much on the equities of a given case as the substance of the legal issues it presents.” *Trump v. Int’l Refugee Assistance Project*, 582 U.S. 571, 579 (2017) (reviewing preliminary injunction). In this case, equitable factors like whether an injunction will pose a serious security threat to tens of millions of users are as relevant as the legal standards for measuring liability under the Sherman Act. On top of that, an aggrieved party is “entitled to have explicit findings of fact upon which the conclusion of the court was based,” *Mayo*, 309 U.S. at 317—and those concerns are heightened when a private-party injunction poses risks for millions of non-parties. Indeed, precisely for these reasons, federal courts are obligated to

make factual findings before issuing preliminary and permanent injunctive relief. Fed. R. Civ. P. 52(a)(1), (2); *see also* Fed. R. Civ. P. 65(d)(1). And those “findings are obviously necessary to the intelligent and orderly presentation and proper disposition of an appeal.” *Mayo*, 309 U.S. at 317.

To make matters worse, the Ninth Circuit explicitly blessed the district court’s failure to make findings on critical issues of computer security affecting millions of users. App.63a-64a. Instead, the Ninth Circuit said it was enough that the district court had before it a “robust record,” App.63a—without any obligation that the district court make findings and draw conclusions based on that record. That, too, violated this Court’s precedents.

Where, as here, “the required findings of fact and conclusions of law have not been set forth,” this Court has held that the injunction “order is invalid.” *Granny Goose Foods*, 415 U.S. at 443 n.17 (explaining the requirement in the context of a preliminary injunction); *accord Purcell v. Gonzales*, 549 U.S. 1, 6 (2006) (per curiam) (vacating injunction where the district court failed to make “any factual findings”). And at least until this case, the Ninth Circuit had not hesitated to vacate injunctions where the district court’s analysis did “not discuss a fact [the court of appeals thought] relevant to weighing the equities.” *E.g.*, *La Quinta Worldwide LLC v. Q.R.T.M. S.A. DE C.V.*, 762 F.3d 867, 880 (9th Cir. 2014); *see also* Arthur R. Miller, *et al.*, 9C Federal Practice and Procedure § 2577 & n.2 (3d ed. 2025) (collecting cases where courts of appeals vacated judgments because district courts had “failed to make findings when they are required by the rule”); *id.* § 2576 (explaining that findings “must be made if

the grant or denial of a permanent injunction turns on issues of fact”).

The requirements of findings of fact and conclusions of law are as much about promoting good process as they are about securing good substance. Procedurally, faithful adherence to these requirements ensures that district courts provide litigants and the public with an explanation for the court’s actions, which, in turn, facilitates appellate review. *Mayo*, 309 U.S. at 317; *see also Purcell*, 549 U.S. at 5 (noting that the absence of findings can deprive the litigants and the public of “the necessity for clear guidance”); 9C Federal Practice and Procedure, *supra*, § 2571 (explaining that findings “afford litigants an understanding of the basis for decision”). Substantively, the requirements of findings and conclusions force district courts to grapple with the relevant issues, which increases the likelihood that the courts will exercise their discretion appropriately. That makes sense. Judges “will give more careful consideration to the problem if they are required to state not only the end result of their inquiry, but the process by which they reached it.” *United States v. Merz*, 376 U.S. 192, 199 (1964).

Here, there is every indication that by declining to make factual findings and draw legal conclusions related to the equities, the district court failed to consider at least three significant shortcomings associated with the relief it ordered:

*First*, even if it were permissible to defer findings to a technical committee, the district court imbued that committee with two serious procedural flaws that will inhibit its ability to guard against the security risks posed by the injunction. To start, the best

security practices are prophylactic and therefore err on the side of protecting users from risks, but before Google may impose security restrictions, it will “bear the burden of proving that its technical and content requirements and determinations are strictly necessary and narrowly tailored.” App. 70a. The district court then left disputes about these issues to the technical committee and gave Google’s adversary, Epic Games, a valuable seat at that three-person table. *See* App.70a-71a. This differs markedly from the process for appointing special masters under Rule 53 of the Federal Rules of Civil Procedure. That rule specifies that a “master must not have a relationship to the parties, attorneys, action, or court that would require disqualification of a judge under 28 U.S.C. § 455, unless the parties, with the court’s approval, consent to the appointment after the master discloses any potential grounds for disqualification.” Fed. R. Civ. P. 53(a)(2). Here, in contrast, the district court baked a conflict into its order over Google’s objection by mandating an Epic-appointed representative to the committee. Epic does not have any incentive to appoint a representative who will act in the best interests of the more than one hundred million Android users based in the United States. Rather, Epic, a privately held company, has a fiduciary obligation to appoint a representative who it believes will act in the best interests of its shareholders.

*Second*, the district court did not make sufficient allowances for the technical committee to review the obvious risks posed by the injunction. The district court did not include any express provision authorizing Google to attempt to screen linkouts from the standpoint of security or safety. App.69a. And the

injunction provides no standards for vetting candidates who request access to Google’s catalog of apps or demand that Google list their app-store app on the Play Store. App.69a-70a. Instead, Google is permitted to impose security and safety standards only on the third-party-app-store *apps* that it is forced to carry on the Play Store. *See id.* Thus, there are glaring gaps in the injunction’s security-review process.

*Third*, no amount of technical guidance can eliminate the risks posed by the injunction. For both linkouts and apps hosted on third-party app stores, Google would need to vet content on external web servers (*e.g.*, developers’ websites, third-party app stores, etc.), which would involve a nearly infinite amount of content at unknown locations. And even if Google could undertake this Herculean task, there’s no reason to believe the web address behind a link or the third-party-app-store app vetted by Google will serve the same content when it is visited at a different time by someone else. For example, one prominent app developer geofenced its app to appear to comply with Apple’s App Store policies when that app detected that it was being run in Cupertino, California (Apple’s headquarters), but it secretly violated those policies when run elsewhere. *The Verge*, *Uber tried to fool Apple and got caught*, Apr. 23, 2017.<sup>17</sup> As this episode illustrates, even if Google could vouch for the content of third-party app stores at some location and moment in time, malicious actors could serve “safe”

---

<sup>17</sup> <https://www.theverge.com/2017/4/23/15399438/apple-uber-app-store-fingerprint-program-tim-cook-travis-kalanick>.

versions of their apps when they are vetted and malicious versions when they are not.

Beyond the risks, there is no obvious benefit to the remedies the district court awarded, underscoring the court's failure to fully assess the equities. Developers are free to communicate directly with potential consumers and make their apps available for download outside of Google's Play Store—without the need for them to embed external links in the apps they make available on the Play Store. And although *amici* are by no means experts on competition law, it is not obvious how consumers are served by allowing anyone on the Internet to free-ride off Google's backend work to prop up an app store—particularly where there are already credible alternatives to the Play Store, including Amazon's Appstore, F-Droid, and Samsung's Galaxy Store (for those with a Samsung device).

Nor are the benefits obvious when the focus is limited to Epic. As *amici* understand it, Epic's principal beef with Google was its policy that all Play Store apps use Google Play Billing—a policy that the district court remedied through other provisions of the injunction. Epic has not shown any need to embed links in apps downloaded on the Play Store or within its Play Store listing. Nor has Epic shown any need to access the entire catalog of Google's Play Store. To the contrary, Epic—one of the largest game developers on the planet—has launched an app store for Android focused exclusively on mobile games, not broader apps unaffiliated with gaming. *See* Epic Games Store,

*Browse* (Filter by Android)<sup>18</sup>; *accord* 5-SER-974; 5-SER-1194.

The upshot is no court has made factual findings related to the risks and potential benefits of the injunction, let alone drawn conclusions based on these factors. This Court’s review is therefore urgently needed to reinforce the vital role these steps play in awarding injunctive relief—particularly injunctive relief that poses a serious threat to the safety and security of millions of non-parties.

### **Conclusion**

The petition for a writ of certiorari should be granted.

Respectfully submitted.

ROBERT T. SMITH  
*Counsel of Record*  
NEAL S. MEHROTRA  
KATTEN MUCHIN ROSENMAN LLP  
1919 Pennsylvania Avenue, N.W.  
Suite 800  
Washington, DC 20006  
robert.smith1@katten.com  
202-625-3500

*Counsel for Amici Curiae*

October 31, 2025

---

<sup>18</sup> <https://store.epicgames.com/en-US/browse?sortBy=releaseDate&sortDir=DESC&tag=Android&count=40&start=0>