

Nos. 24-6256, 24-6274

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION

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
The Honorable James Donato

**BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER
FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLEE
EPIC GAMES, INC. AND AFFIRMANCE**

Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: mitch@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Dated: January 7, 2025

By: /s/ Mitchell L. Stoltz
Mitchell L. Stoltz

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT	i
TABLE OF CONTENTS	ii
TABLE OF AUTHORITIES	iii
STATEMENT OF INTEREST OF AMICUS	1
ARGUMENT	3
I. THE SECURITY OFFERED BY A MONOPOLIST IS MORE FRAGILE THAN WHAT A COMPETITIVE MARKET CAN PROVIDE.....	3
II. THE ANTITRUST LAWS FORECLOSE GOOGLE’S ARGUMENT THAT MONOPOLY IS BETTER FOR CONSUMERS THAN COMPETITION.	7
III. IN A COMPETITIVE MARKET, BOTH GOOGLE AND COMPETING APP DISTRIBUTORS CAN MITIGATE SECURITY RISKS.....	9
CONCLUSION	12
CERTIFICATE OF COMPLIANCE	13
CERTIFICATE OF SERVICE.....	14

TABLE OF AUTHORITIES

Cases

<i>Epic Games, Inc. v. Apple, Inc.</i> , 67 F.4th 946 (9th Cir. 2023)	9
<i>F.T.C. v. Indiana Fed’n of Dentists</i> , 476 U.S. 447 (1986)	9
<i>Nat’l Soc’y of Professional Engineers v. United States</i> , 435 U.S. 679 (1978)	8

Other Authorities

“EFF Urges FTC to Address American Resellers of Malware on Android TV Set- Top Boxes,” Press Release (Nov. 14, 2023)	2
“Reject Nevada’s Attack on Encrypted Messaging, EFF Tells Court,” Press Release (March 12, 2024)	1
Alexis Hancock, “Low Budget Should Not Mean High Risk: Kids’ Tablet Came Preloaded With Sketchyware,” EFF Deeplinks Blog (Nov. 14, 2023)	1
Alison Dame-Boyle, “EFF at 25: Remembering the Case that Established Code as Speech,” EFF Deeplinks Blog (April 16, 2015)	1
Bill Budington, “Anatomy of an Android Malware Dropper,” EFF Deeplinks Blog (April 4, 2022)	2
Bill Toulas, “Android malware infiltrates 60 Google Play apps with 100M installs,” Bleeping Computer (April 15, 2023)	6
Bruce Schneier, “You Have No Control Over Security on the Feudal Internet,” Harvard Business Review (June 6, 2013)	3, 4
Camilla Palladino, “It’s not just CrowdStrike—the cyber sector is vulnerable,” Financial Times (July 19, 2024)	5
Certbot	1
Competition	2
Gennie Gebhart, “Dark Caracal: Good News and Bad News,” EFF Deeplinks Blog (January 19, 2018)	2
Jinson Varghese, “iOS vs Android Security: A Comprehensive Comparison,” Astra (June 30, 2024)	6

Lily Hay Newman, “How One Bad CrowdStrike Upgrade Crashed the World’s Computers,” Wired (July 19, 2024).....	5
Privacy Badger	1
Reproducible Builds	4
ZScaler ThreatLabz, “2024 Mobile, IoT, & OT Threat Report”	5, 6

STATEMENT OF INTEREST OF AMICUS¹

The Electronic Frontier Foundation (“EFF”) is a non-profit civil liberties organization based in San Francisco, California, and supported by over 33,000 dues-paying members. EFF has worked for over 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. Protecting the security and privacy of technology users is at the heart of EFF’s work. EFF has long fought for users’ rights to use encryption and other privacy-enhancing technologies.² EFF itself develops such technologies, such as Privacy Badger and Certbot, and distributes them at no charge.³ EFF also strives to protect users from malware by investigating and reporting on dangerous consumer products, including mobile apps.⁴

¹ Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amicus certifies that no person or entity other than amicus curiae, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

² Alison Dame-Boyle, “EFF at 25: Remembering the Case that Established Code as Speech,” EFF Deeplinks Blog (April 16, 2015), at <https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech> (describing the 1995 case of *Bernstein v. U.S. Department of Justice*); “Reject Nevada’s Attack on Encrypted Messaging, EFF Tells Court,” Press Release (March 12, 2024), at <https://www.eff.org/press/releases/reject-nevadas-attack-encrypted-messaging-eff-tells-court>.

³ “Privacy Badger,” <https://www.eff.org/pages/privacy-badger>; “Certbot,” <https://certbot.eff.org/>.

⁴ See, e.g., Alexis Hancock, “Low Budget Should Not Mean High Risk: Kids’ Tablet Came Preloaded With Sketchyware,” EFF Deeplinks Blog (Nov. 14, 2023),

EFF also recognizes that market concentration in information technology markets, combined with the efforts of major consumer technology platforms to maintain their dominance of key markets, deprives users of control over their own vital technological tools, including mobile phones and other computing devices, and ultimately harms users' privacy, security, and autonomy.⁵

INTRODUCTION

The district court's injunction is crafted to enable a competitive marketplace for Android app distribution, remedying Google's app distribution monopoly. Robust competition among Android app stores will enhance the security and privacy of Android users by clearing the way for competing app stores that offer *greater* security than the Google Play Store provides.

Google and several of its amici assert that the injunction will harm users' security because Android users, the majority of whom get their apps from the

at <https://www.eff.org/deeplinks/2023/11/low-budget-should-not-mean-high-risk-kids-tablet-came-preloaded-sketchyware>; "EFF Urges FTC to Address American Resellers of Malware on Android TV Set-Top Boxes," Press Release (Nov. 14, 2023), at <https://www.eff.org/press/releases/eff-urges-ftc-address-american-resellers-malware-android-tv-set-top-boxes>; Bill Budington, "Anatomy of an Android Malware Dropper," EFF Deeplinks Blog (April 4, 2022), at <https://www.eff.org/deeplinks/2022/04/anatomy-android-malware-dropper>; Gennie Gebhart, "Dark Caracal: Good News and Bad News," EFF Deeplinks Blog (January 19, 2018), at <https://www.eff.org/deeplinks/2018/01/dark-caracal-good-news-and-bad-news> (report describing a family of malware distributed through the Google Play Store).

⁵ "Competition," <https://www.eff.org/issues/competition>.

Google Play Store, will encounter third-party app stores and apps not vetted by Google. They are correct—to a point. Changes to an important computing environment create security risks as users adapt. Ultimately, though, competitive markets serve users’ needs better than monopolies, and security is no exception. This is more than just empirical fact—it’s the law. Google’s argument that its monopoly over Android app distribution serves consumers better than a court-ordered transition to competition is wrong, and is foreclosed by the antitrust laws. The injunction permits Google an appropriate role in vetting apps and app stores, while also empowering competitors to pursue *better* vetting. In short, while it must be implemented carefully, the injunction serves the public’s interest in security.

ARGUMENT

I. THE SECURITY OFFERED BY A MONOPOLIST IS MORE FRAGILE THAN WHAT A COMPETITIVE MARKET CAN PROVIDE.

Users of mobile computing devices have come to expect that their security is someone else’s responsibility. As security expert Bruce Schneier wrote, “[t]he new security model is that someone else takes care of it—without telling us any of the details.”⁶ This approach has benefits, including cost, reliability, and frequently, security itself. But this is inherently a feudal relationship, in which users “cede

⁶ Bruce Schneier, “You Have No Control Over Security on the Feudal Internet,” Harvard Business Review (June 6, 2013), available at <https://hbr.org/2013/06/you-have-no-control-over-s>.

control of [their] data and computing platforms to these companies and trust that they will treat [them] well and protect [them] from harm.”⁷

Feudal security has important limitations. Firms that have assumed control over users’ security can make mistakes that compromise that security. They can act arbitrarily and change policies without user consent or input. And they use various techniques, including the contractual arrangements at issue in this case, to lock users into their platform and limit consumer choice.⁸

Google’s control over the Android computing environment through its Play Store monopoly is a premier example of feudal security. Google reviews apps for safety and reliability and removes malicious and faulty apps from the Play Store. But Android users have little visibility into this process. And because, as the jury found, Google’s agreements restrain trade among Android app stores, users are denied access to alternatives that could do a *better* job of vetting apps, or apply more restrictive criteria for app safety and reliability. For example, a competing app store could offer apps whose code is independently verifiable.⁹

The concentration of the Android app distribution market as a result of Google’s illegally maintained monopoly power also creates a security

⁷ *Id.*

⁸ *See id.*

⁹ *See* Reproducible Builds, <https://reproducible-builds.org/>.

“monoculture” in which lapses by a single firm could leave millions of users vulnerable. The security consequences of market concentration can be dire. In July 2024, an error in a software upgrade sent by the widely used cybersecurity software provider CrowdStrike caused outages around the world, including of critical systems used by hospitals, airlines, and emergency responders.¹⁰ CrowdStrike was one of three firms that collectively controlled over 50% of the market for “endpoint” security monitoring software, and the incident raised concerns about market concentration among cybersecurity firms.¹¹ The same concern applies to Google’s Play Store. Because Android apps potentially have access to personal data on those devices, including user input, incoming messages, and banking credentials,¹² even a subtle and inadvertent error by Google could leave millions vulnerable.

Indeed, this happens regularly. A recent study by threat analysts at Zscaler ThreatLabz found over 200 malicious applications that were available for download at the Google Play Store over a one-year period, which were collectively

¹⁰ Lily Hay Newman, “How One Bad CrowdStrike Upgrade Crashed the World’s Computers,” *Wired* (July 19, 2024), at <https://www.wired.com/story/crowdstrike-outage-update-windows/>.

¹¹ Camilla Palladino, “It’s not just CrowdStrike—the cyber sector is vulnerable,” *Financial Times* (July 19, 2024), at <https://www.ft.com/content/d2f529fe-3050-4ef5-a8c7-6487d533e57a>

¹² ZScaler ThreatLabz, “2024 Mobile, IoT, & OT Threat Report” at 15, available at <https://www.zscaler.com/campaign/threatlabz-mobile-iot-ot-report>.

installed by users nearly 8 million times.¹³ Another study identified malware embedded in a software library that was unknowingly used by the developers of 60 apps distributed through the Play Store, resulting in over 100 million downloads.¹⁴

Better vetting of apps to avoid these threats is achievable. For example, the prevalence of malware on Apple's iOS platform is generally believed to be lower than on Android, due in part to Apple's more thorough vetting process.¹⁵ Competing Android app stores, given a meaningful opportunity to serve the market of Android users, could also achieve a safer catalog of apps, with less malware, creating a competitive advantage and putting pressure on Google to improve its own vetting.¹⁶

The current lack of meaningful competition for app distribution in the Android market means that the level of security Google currently offers is not guaranteed. Changes to Google's commercial priorities could cause the number of malicious apps distributed through the Play Store to increase, and Google's market

¹³ *Id.* at 17.

¹⁴ Bill Toulas, "Android malware infiltrates 60 Google Play apps with 100M installs," Bleeping Computer (April 15, 2023), at <https://www.bleepingcomputer.com/news/security/android-malware-infiltrates-60-google-play-apps-with-100m-installs/>.

¹⁵ *See, e.g.*, Jinson Varghese, "iOS vs Android Security: A Comprehensive Comparison," Astra (June 30, 2024), at <https://www.getastra.com/blog/mobile/ios-vs-android-security/>.

¹⁶ *See* Reproducible Builds, *supra* n. 9.

power in app distribution means that Google would face little or no competitive pressure to avoid that outcome.

In short, the feudal security offered by Google is often effective, but its effectiveness is conditional and fragile. A meaningful choice of alternative app stores, enabled by the injunction in this case, would allow the market to deliver better security to more users in more circumstances.

II. THE ANTITRUST LAWS FORECLOSE GOOGLE’S ARGUMENT THAT MONOPOLY IS BETTER FOR CONSUMERS THAN COMPETITION.

Google and several of its amici argue that the injunction will harm consumers by exposing them to more malicious software, but the real target of their argument is not the injunction but competition itself.

Google objects to the injunction language that permits it to “take reasonable measures to ensure” that third-party app stores distributed through the Play Store meet Google’s standards for content, as long as those measures are “strictly necessary and narrowly tailored.” The injunction would not prevent Google from banning an app store that offered malicious apps from distribution in the Play Store. And the injunction does not require *ex ante* permission for such banning—Google could ban such stores as soon as the threat is known, as long as it is prepared to justify that action later if challenged. Because the injunction permits Google to ban apps and app stores appropriately on a case-by-case basis, Google is

effectively asserting that any constraint on its unilateral judgment on security issues is intolerable.

Google’s amici likewise decry open competition in app distribution as inherently unsafe. John Mitchell *et al.* argue that the injunction “would make it too easy for people to set up an app store.” Brief of Computer Security Experts John Mitchell *et al.* at 30. The brief of former national security officials similarly asserts that “smaller third-party app stores” may not be “willing or able” to review apps for malicious behavior. Brief of Former National Security Officials at 18-19.

These arguments are “nothing less than a frontal assault on the basic policy of the Sherman Act.” *Nat’l Soc’y of Professional Engineers v. United States*, 435 U.S. 679 (1978). As the Supreme Court has held,

The assumption that competition is the best method of allocating resources in a free market recognizes that all elements of a bargain—quality, service, *safety*, and durability—and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers. Even assuming occasional exceptions to the presumed consequences of competition, the statutory policy precludes inquiry into the question whether competition is good or bad.

Id. (emphasis added). The Court further held that neither alleged concern for public safety nor the possibility of competitors acting unethically provide “a reason, cognizable under the Sherman Act, for doing away with competition.” *Id.* at 696. Subsequent cases confirmed that “a defendant cannot severely limit interbrand competition on the theory that competition itself is ill-suited to a certain market or

industry.” *Epic Games, Inc. v. Apple, Inc.*, 67 F.4th 946, 988 (9th Cir. 2023) (collecting cases).

The agreements at issue in this case limit Android users’ access to information about app security and privacy that competing app stores seek to give consumers—judgments that may differ from Google’s in important ways. Google and its amici argue in effect “that an unrestrained market in which consumers are given access to the information they believe to be relevant to their choices will lead them to make unwise and even dangerous choices,” an argument the Sherman Act forecloses. *F.T.C. v. Indiana Fed’n of Dentists*, 476 U.S. 447, 463 (1986).

While these precedents deal with the rule of reason analysis for antitrust liability, their logic extends to remedies. They imply that an injunctive remedy to an antitrust violation is not invalid simply because it will increase competition that a defendant believes is harmful.¹⁷

III. IN A COMPETITIVE MARKET, BOTH GOOGLE AND COMPETING APP DISTRIBUTORS CAN MITIGATE SECURITY RISKS.

The risks inherent in the transition from monopoly to effective competition

¹⁷ This case differs from *Epic Games Inc. v. Apple Inc.*, in which this Court found that interbrand competition (between Apple and Google) justified Apple’s restraints on competition on its own devices. *Apple*, 67 F.4th at 989. This case concerns interbrand competition between Google and other app store providers. The jury considered and rejected Google’s defenses regarding competition with Apple.

in Android app distribution, enabled by the injunction, do not invalidate the injunction, because those risks are themselves a result of Google’s illegal conduct, are transitory, and can be mitigated.

The harms identified by Google and its amici, while significant, are fundamentally *misattributions of responsibility* for users’ security. Android is already an open platform in which users can access alternative app stores or “sideload” apps from the internet. Appellant’s Opening Br. 9; 5-ER-983. Android contains warnings to users about installing and running untrusted applications, but the choice to do so, and the attendant risks of malware, invasions of privacy, unwanted content, and poor quality have always laid with users.

The injunction shifts the bounds of Google’s responsibility for security. It requires Google to increase users’ access to third-party app stores within the Google Play platform, to remedy Google’s illegal conduct by giving competing stores an opportunity to achieve scale. Under the injunction, while Google will retain the ability to vet third-party apps and app stores for security when including them in the Play Store, third-party stores will continue to have a more direct responsibility for the security of users who choose to use them. Google complains that “requiring [it] to distribute third-party app stores risks subjecting Play users to stores that distribute pirated, unsafe, or inappropriate content.” Appellants’ Opening Brief at 82-83. But Play users are already subjected to these risks, if and

when they choose to sideload apps or install third-party app stores, having acknowledged the risks when warned by Android.

Users' current expectations are a byproduct of Google's monopoly over Android app distribution. John Mitchell *et al.* observe that users may have a false sense of security concerning apps downloaded from the Play Store once, under the injunction, those apps can contain links to externally hosted software or can be app stores themselves.¹⁸ This is true, but users' beliefs about security arose in a world where Google distributed the vast majority of Android apps installed on devices—a world made possible by the conduct the jury found illegal. If Android users currently believe that only Google can ensure their security, that belief is itself a symptom of Google's illegally maintained monopoly, because most consumers had no meaningful choice aside from trusting Google.

Users' expectations can and will shift as competition increases. The injunction does not bar Google from warning users when they leave the bounds of Google's curated garden by following links to externally hosted apps or by using third-party app stores, nor from educating users in other ways. In fact, Google would be acting irresponsibly if it did not give such warnings. And moreover, once consumers understand that Google is no longer the feudal guarantor of their security when they cross those bounds, they will be empowered to choose the app

¹⁸ Brief of John Mitchell et al. at 12.

stores that best serve their needs.

Google and others can mitigate these transitional risks through careful design and user education, neither of which are foreclosed by the injunction. Rather, the injunction simply provides for external review of Google's security decisions via the technical committee, to discern—after the fact if necessary—whether security rationales for excluding an app store are real or pretextual.

CONCLUSION

The transition to a competitive market for Android app distribution does involve risks. But as the jury found, the current market is not serving consumers. Both factually and as a matter of legal policy, competition will deliver better security and privacy to users. Accordingly, this Court should not be swayed to abandon the goal of a competitive market by the fearmongering of Google and its amici.

Dated: January 7, 2025

By: /s/ Mitchell L. Stoltz
Mitchell L. Stoltz
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
mitch@eff.org

*Counsel for Amicus Curiae
Electronic Frontier Foundation*

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiff–Appellee Epic Games, Inc. and Affirmance with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 2,617 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point Times New Roman font.

Dated: January 7, 2025

By: /s/ Mitchell L. Stoltz
Mitchell L. Stoltz

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that 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 on January 7, 2025.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: January 7, 2025

By: /s/ Mitchell L. Stoltz
Mitchell L. Stoltz

Counsel for Amicus Curiae