No. 21-16506 and 21-16695

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

EPIC GAMES, INC.,

PLAINTIFF, COUNTER-DEFENDANT - APPELLANT, CROSS - APPELLEE

v.

APPLE INC.,

DEFENDANT, COUNTERCLAIMANT – APPELLEE, CROSS-APPELLANT

On Appeal from the United States District Court
for the Northern District of California
20-cv-05640-YGR-TSH
The Honorable Yvonne Gonzalez Rogers

BRIEF OF AMICUS CURIAE THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT, CROSS-APPELLEE EPIC GAMES AND REVERSAL

Mitchell L. Stoltz
Counsel of Record
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 states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Dated: January 27, 2022

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF AMICUS[1]

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization with more than 38,000 dues-paying members. EFF has worked for over 30 years to ensure that technology supports freedom, justice, and innovation for all the people of the world.

INTRODUCTION AND SUMMARY

A central function of the antitrust laws is to keep markets free from restraint so that the benefits of innovation can reach consumers. The district court's findings of fact rightly recognized that Apple's restrictive App Store policies—its exclusive control over app distribution and vetting on Apple devices and its requirement that app developers use Apple's own in-app payment service—have significant anticompetitive effects, including the prevention of innovative and improved app distribution methods. But in upholding Apple's restraints, the district court erred in at least three respects.

First, the district court erred in its legal analysis of the existence and competitive state of aftermarkets for app distribution and in-app payment services, relying on an unsupported legal presumption that Apple device users have full

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amicus* certifies that no person or entity, other than amicus, 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.

information about, and meaningfully understand, Apple's policies when they commit themselves to Apple's platform. The court thus erred in finding that competition in the foremarket for smartphones disciplined competition in aftermarkets for app distribution and in-app payment services.

Second, the court erred in finding that app distribution and in-app payments were a single product, given the independent demand for each and the existence of alternatives on platforms that are free of Apple's restrictive policies.

Third, the court did not weigh Apple's rationales for its policies—particularly, the company's argument that its restrictions improve users' information security and privacy—against the anticompetitive effects it found, as the Sherman Act requires. The court erred by treating Apple's security rationale as conclusive, instead of recognizing that a dominant firm's supplanting market forces with its own security and privacy decisions is anticompetitive—not procompetitive—and forecloses innovation.

Reversing these errors, and finding Apple's restrictive policies illegal under the rule of reason, will unlock innovation across the mobile app world, including innovations in app distribution, payments, security, and privacy. Allowing these innovations to reach consumers and thrive in the market regardless of whether they come from Apple, its favored partners, or independent sources would benefit all users and developers of mobile technology.

I. Commercial Realities Support Epic's Proffered Market Definition, Including Aftermarkets for App Distribution and In-App Payments.

The district court's decision to define a mobile gaming transactions market—without regard to how the markets for smartphones and operating systems impact that market—is contrary to the law, the evidence, and the realities of mobile software distribution. Its fatal flaw is that it relies on an unsupported legal presumption, namely that consumers have knowledge of Apple's restrictions and, therefore, the distribution market is competitive. Further, because purchasers of smartphones cannot effectively evaluate the costs of apps over the lifetime of a device—much less how Apple's restrictions impact those costs—the court's rejection of Epic's proffered aftermarkets was error. Relatedly, the court's rejection of an in-app purchase (IAP) aftermarket in reliance on *Ohio v. American Express Co.*, 138 S. Ct. 2274 (2018) ("*Amex*"), is not supported by that or any other decision regarding two-sided platforms.

A. A Single-Brand Aftermarket Is Appropriate Whenever Aftermarket Restraints Are Not Disciplined By Foremarket Competition—Even If Customers Are Aware of the Restraints.

In rejecting a distribution aftermarket, the court held that a lack of evidence "that consumers *are unaware* that the App Store is the sole means of digital distribution on the iOS platform" precluded the existence of an aftermarket. 1-ER-134. This holding is based on the court's presumption that, if consumers are aware of a restriction when purchasing a device (and operating system), then competition

in that market is sufficient to discipline Apple's anticompetitive restrictions in the derivative distribution market and iOS users are not subject to lock-in effects. *Id.*

That conclusion is inconsistent with Supreme Court and Ninth Circuit precedent. A single-brand aftermarket is appropriate where "market imperfections, including information and switching costs, prevent[] consumers from discovering, as they [are] shopping for equipment, that the [defendant's] brand would include a de facto commitment to consume only supracompetitively priced" goods or services in a derivative market. *Newcal Indus., Inc. v. Ikon Office Solution*, 513 F.3d 1038, 1048 (9th Cir. 2008) (citing *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 473-78 (1992)). In other words, an aftermarket definition is appropriate if "[c]ompetition in the initial market . . . does not necessarily suffice to discipline anticompetitive practices in the aftermarket." *Id.* at 1050.

Accordingly, the court should have assessed whether competition in the market for smartphones and operating systems might discipline Apple's restrictions on app distribution. Instead, the court *assumed* the existence of that competition based on *the possibility* that consumers might be aware of Apple's restrictions. Such presumptions based on "formalistic distinctions rather than actual market realities" are disfavored under the antitrust laws. *Eastman Kodak*, 504 U.S. at 466-67. Moreover, the court applied that presumption in the face of substantial evidence that consumers cannot effectively internalize a device's lifecycle costs from apps when

purchasing a device, that switching costs are substantial, that competition in the device-operating system market is lacking, and that Apple has market power in the duopoly operating system market. *See* 1-ER-134; Findings of Fact & Conclusions of Law Proposed by Epic Games, Inc. ¶¶ 166-178.[2]

B. Customers Do Not and Cannot Internalize App Costs When Buying an Apple Device.

The commercial realities of app distribution (and common sense) demonstrate that consumers cannot effectively internalize app costs. Thus, competition in the device operating-system market does not discipline Apple's anticompetitive restrictions on app distribution. Several factors (in addition to evidence adduced by Epic at trial) prevent competition in the device operating-system market from forcing Apple to remove its anticompetitive restraints or reduce its supracompetitive commissions:

First, Apple's restrictions most directly impact app developers, who pay Apple's supracompetitive commission. 1-ER-35–36, 102. As the district court

[2] In rejecting evidence of high switching and information costs, the district court relied on evidence of competition from non-mobile gaming platforms (even though the court rejected Apple's proffered market definition including all forms of gaming) and the incipient development of cross-platform gaming. 1-ER-133–34. This conclusion is at odds with the fact that "mobile gaming [is] a distinct market within the wider video gaming market" focused on casual gamers and with the court's own statement that "games are, for the most part, cabined to certain platforms" and that cross-platform play is largely limited to Fortnite and Minecraft. 1-ER-75–76, 87. The vast majority of developers' games in the App Store are not available for cross-platform play.

recognized, the App Store is a two-sided platform. 1-ER-124. This allows Apple to impose supracompetitive costs to developers that are only indirectly felt by consumers. *See* 1-ER-102, 147. As a result, even if a consumer has perfect information about current and future app prices and costs (an impossibility), the consumer cannot know the degree to which Apple's restrictions raise app prices. A consumer would need econometric evidence of the degree to which developers pass on Apple's supracompetitive commissions to understand how much they are overpaying by choosing a particular operating system.

Second, no consumer, as a practical matter, can accurately assess at the time of purchase their unique lifecycle costs from apps for a particular device.[3] Consumers have only an incomplete conception of the apps they expect to use and how much they will use them. A user will not know what apps are available over the life of a device, much less which they will decide to spend money on, and an individual's preferences for apps are often in flux.[4] Moreover, consumers typically

[3] "Lifecycle pricing of complex, durable equipment is difficult and costly. In order to arrive at an accurate price, a consumer must acquire a substantial amount of raw data and undertake sophisticated analysis. . . . . Much of this information is difficult—some of it impossible—to acquire at the time of purchase. During the life of a product, companies may change . . . prices, and develop products with more advanced features . . . . In addition, the information is likely to be customer-specific; lifecycle costs will vary from customer to customer . . . ." *Eastman Kodak*, 504 U.S. at 473-74.

[4] Over 2 million new apps and games were launched across both iOS and Android in 2021. *The State of Mobile 2022*, App Annie, https://www.appannie.com/en/go/state-of-mobile-2021/ (discussing consumer app

do not engage in that kind of sophisticated analysis. Instead, the decision to purchase a device is intuitive and often based on appearance, technical features, and peer influence.[5]

Third, consumers purchasing a device must assess a multitude of device characteristics and other considerations, meaning that even if a consumer could accurately determine its anticipated lifecycle app costs, those costs are only one factor among many to be considered. Consumers purchase and use smartphones for many functions.[6] Where consumers must decide whether to purchase an item based

---

download trends in gaming, retail, banking, and other segments) (last visited Jan. 27, 2022). On iOS, over 6 million apps have been released since the launch of the App Store, and 1.8 million apps are currently available for download. *Id.*

[5] University of Seville, *Consumers choose smartphones mostly because of their appearance*, ScienceDaily (Oct. 18, 2018), https://www.sciencedaily.com/releases/2018/10/181018105330.htm (reviewing study analyzing myriad factors influencing purchasing decision with aesthetic factors dominating); *see also* 1-ER-48 ("Competition exists for smartphones which are more than just the operating system. Features such as battery life, durability, ease of use, cameras, and performance factor into the market." (citations omitted)), 54 n. 269 ("Consumers who switched from Android to iOS did so for hardware reasons, such [as] 'speed,' 'quality device construction,' and 'battery'—not app quality, price, or availability. This reinforces Dr. Evans' point that apps are a secondary consideration when purchasing a smartphone and would not lead to switching by themselves."); Nicholas De Leon & Melanie Pinola, *Best Smartphones of 2022*, Consumer Reports (Jan. 1, 2022), https://www.consumerreports.org/smartphones/best-smartphones-of-the-year-a7852223918/ (discussing various features of top smartphones, including camera quality, battery life, and price, without reference to apps or app costs).

[6] Without the use of any third-party software, most or all smartphones can place telephone calls, send and receive text messages, save and maintain contacts, take photographs or videos, save files, keep a calendar, and tell time, among many other

on many factors, research shows that decisionmakers favor easily retrievable and understood preferences over questions that are difficult to quantify.[7] And where the ability (or cost) to acquire information for a purchase decision is difficult (or expensive) relative to the savings from acquiring that information, consumers do not acquire that information, limiting competition.[8]

Fourth, characteristics of device operating-system markets prevent consumers from incorporating app costs into their decision-making. Because the overwhelming majority of mobile devices run either iOS or Android, the vast majority of third-party apps are available on all mobile devices at similar, if not identical, prices. *Cf.* 1-ER-55 ("Most popular mobile games are available on both Android and iOS, with

---

functions. Third-party apps allow for innumerable additional functions. A prospective smartphone purchaser may also assess the physical design and functioning of the hardware, the design and functioning of the operating system, the handset and operating system's integration with other hardware and software, the life expectancy of the device, costs to repair, and price. A consumer's decision to purchase a particular brand and model of handset imperfectly assesses all or some of these factors.

[7] *See* Daniel Kahneman & Shane Frederick, *Representativeness revisited: Attribute substitution in intuitive judgment*, *in Heuristics & Biases: The Psychology of Intuitive Judgment* (ed. T. Gilovich et al.) (2002) ("[W]hen confronted with a difficult question people often answer an easier one instead."). Unlike console games, where consumers purchase a console and use the platform primarily for the purposes of playing games, mobile games are only one of many uses for, and reasons for purchasing, a smartphone. Competition in the foremarket for consoles would thus have a greater disciplining effect on aftermarket restrictions. *But see* 1-ER-135 n. 588.

[8] *See* George J. Stigler, *The Economics of Information*, 69 J. of Pol. Econ. 213 (1961).

similar functionality. . . . [A] significant difference in game transaction price or availability does not exist between iOS and Android."). This means that a rational consumer should in fact *disregard* the cost of apps in deciding what device to purchase. This prevents app distribution costs from providing any discipline in the device (and operating system) market.

C. In-App Payments Constitute an Aftermarket Regardless of Whether the App Store is a Two-Sided Market.

The court's holding rejecting an IAP aftermarket, derivative of a distribution market, also lacks support. The court held that an "aftermarket approach to market definition is inconsistent with" the App Store's classification as a two-sided transaction platform. 1-ER-130. Putting aside whether the App Store is indeed a transaction platform, there is no basis under *Amex* (or any other decision) for concluding that a two-sided platform cannot have a derivative aftermarket. *See generally Amex*, 138 S. Ct. at 2280 ("[A] two-sided platform offers different products or services to two different groups who both depend on the platform to intermediate between them."). Other than the requirement that both sides of the platform be considered, there is no reason to assume that a two-sided platform should not be analyzed like any other market. Indeed, at least one circuit court has analyzed a market at least partly derivative of a two-sided platform. *See Viamedia, Inc. v. Comcast Corp.*, 951 F.3d 429, 439, 442 (7th Cir. 2020) (analyzing claims of monopolization of the "advertising representation services market," which provide

services including "[i]nterfacing with the relevant Interconnect[s]," which are two-side platforms). As there is no basis in law for rejecting such a derivative market, the evidence supports the existence of a derivative IAP aftermarket.

II. App Distribution and In-App Payments Are Separate Products

The district court's rejection of Epic's tying claim, specifically its holding that app distribution and IAP are not separate products, is similarly flawed. As discussed above, the *Amex* decision provides no support for this holding. The district court's holding also contains other legal errors.

First, the court misapplied the *Jefferson Parish* standard. Although the court recognized that the question of two separate products "turns not on the functional relationship between them," *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 19 (1984), the court's holding is based on two factual findings, one of which is based on "the functional relation between" distribution and IAP—that is, "the IAP system is integrated into the iOS devices." 1-ER-156-57. Thus, the court based its holding, at least in part, on the functional relationship between distribution and IAP.

In purportedly assessing the existence of separate consumer demand, the court misapprehends the nature of IAP, which is primarily a payment processing function. The court found that IAP "is a secured system which tracks and verifies digital purchases" and "collects the appropriate commission;" it "records all digital sales by identifying the customer and their payment methods," "conducts fraud-related

checks," and "provides information to consumers so that they can view their purchase history, share subscriptions . . . , manage spending, and challenge and restore purchases." 1-ER-68. These characteristics are the kinds of services provided by other payment processing service providers,[9] and are similar to the services provided by digital wallets, like Apple Pay and Google Pay.[10] A competitive advantage to Apple from integrating its IAP with iOS is not a basis for holding that demand is not distinct between IAP and distribution.

The court's holding that distribution and IAP are not separate products is also inconsistent with the development of other software markets that are not controlled by Apple. For instance, in the context of software distribution for PC and Mac computers, there are multiple ways to pay additional charges for add-on features. While some gaming platforms bundle distribution with in-game purchases, there are many software applications and games, including mobile applications, that process in-software purchases through the software itself—that is, separate from distribution—including through reliance on third-party payment processors.[11]

---

[9] Katie Horne, *8 Ways to Accept Online Payments in 2022*, Digital, https://digital.com/online-payment-processing-providers/ (last updated Nov. 26, 2021).

[10] *See, e.g.*, *Apple Pay*, https://www.apple.com/apple-pay/ (last visited Jan. 27, 2022).

[11] Jennifer Mendez, *Top 5 Payment Processors in the Games Industry*, Black Shell Media (July 9, 2017), https://blackshellmedia.com/2017/07/09/top-5-payment-processors-games-industry/.

III. Weighing the Record as Required Under the Rule of Reason, the Court Should Find That Apple's Security Justification Does Not Overcome the Anticompetitive Effects of its App Store Policies.

The district court's rule-of-reason analysis was flawed, because it treated Apple's portrayal of the security and privacy impacts of the App Store policies as conclusive. The court's findings of fact show that Apple's approach to security is itself anticompetitive. Even after accepting Apple's security rationale as a procompetitive justification, the district court should have finished the rule-of-reason analysis by weighing the procompetitive and anticompetitive effects of Apple's policies. *See Fed. Trade Comm'n v. Qualcomm Inc.*, 969 F.3d 974, 991 (9th Cir. 2020) (citing *U.S. v. Microsoft Corp.*, 253 F.3d 34, 58-59 (D.C. Cir. 2001)); *L.A. Mem'l Coliseum Comm'n v. NFL*, 726 F.2d 1381, 1391 (9th Cir. 1984). In properly conducting the rule-of-reason analysis under §§ 1 and 2 of the Sherman Act, this Court should find that the anticompetitive effects of Apple's policies outweigh Apple's proffered justifications.

The record, viewed in its entirety, shows that Apple's security rationale is weak and does not overcome the harm its policies cause to innovation, including innovation that would enhance consumers' security and privacy.

The district court found that the restrictions Apple imposes on app developers have substantial anticompetitive effects. 1-ER-98–106, 147–48. Apple restricts iPhones and other iOS devices to loading apps only from Apple's own App Store.

1-ER-95–96. Apple also exercises strict control over the third-party apps it allows to be distributed through the App Store: the company places restrictions on both the functionality and the expressive contents of apps, and refuses or delists apps that transgress these restrictions. 1-ER-111–13. Apple also requires that app purchases and in-app payments use Apple's own payment systems, an arrangement that allows Apple to collect supra-competitive commissions on such transactions. 1-ER-38–39. The district court found that these policies foreclose competition from other app stores, increase prices for developers, and reduce innovation. 1-ER-98–106. These findings, wrote the district court, were evidence of anticompetitive effects. 1-ER-148.[12]

The district court then addressed Apple's justifications for its restrictions on app distribution and payment processing. Apple argued that the restrictions "help[] ensure a safe and secure ecosystem." 1-ER-107. With respect to Apple's security rationale, the court also evaluated alternatives suggested by Epic, including a "notarization" approach that would allow Apple to continue reviewing apps for security and safety while still enabling app distribution through alternative channels,

[12] The district court's findings echo concerns *amicus* raised about Apple's platform as early as ten years ago: that iOS devices are "beautiful crystal prisons" that limit the innovation available to users of the platform. *See* Micah Lee and Peter Eckersley, *Apple's Crystal Prison and the Future of Open Platforms*, EFF Deeplinks Blog (May 29, 2012), https://www.eff.org/deeplinks/2012/05/apples-crystal-prison-and-future-open-platforms.

such as competing app stores. 1-ER-115–16. Apple uses the notarization approach on its Mac computers, albeit with a lower level of app review. *Id.*

In light of these findings, the district court's legal conclusions on Apple's proffered security justifications went wrong in four ways.

A. Different Consumers Have Different Security Needs, And Apple's Policies Stop the Market from Addressing Consumer Demand for Security.

Security and privacy are elements of competition, not extraneous to the competitive process. Thus, measures that a firm takes to improve customers' security and privacy can themselves be procompetitive or anticompetitive. Of course, such measures only support a rule-of-reason defense if they are in fact procompetitive. As the Supreme Court has held, the policy behind the antitrust laws is 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." *Nat'l Soc. of Pro. Engineers v. United States*, 435 U.S. 679, 695 (1978) (emphasis added).

"Security" means different things for different market participants, and these differences are key to evaluating whether a security rationale is in fact procompetitive. The district court noted that Epic defined security as "preventing an app from performing unauthorized actions or stealing user data," 1-ER-108, while Apple took an expansive view that encompassed Apple's judgment about the

"quality" of apps—notably including Apple's judgment on whether the expressive content of an app is "objectionable." 1-ER-111–13. This divergence of views occurs not just between the parties to this lawsuit but across the spectrum of demand for mobile apps. The district court's findings suggest that Apple's policies have limited the market's ability to provide for these varying needs—in other words, the policies are anticompetitive, even if they are done for reasons of security.

Information security professionals use "threat modeling" to improve the security of software.[13] One common approach to threat modeling is to identify different populations of technology users, identify the specific threats those users face and the risks they present, and then weigh the costs and effectiveness of the various means of mitigating those risks.[14]

For some users, the greatest need is to shield data and communications from eavesdroppers, whether an abusive partner, corporate espionage, or a repressive government. *Id.* These users may need access to apps that provide secure communications, such as virtual private network (VPN) apps or encrypted messaging. Other users may need the broadest possible access to information, such

---

[13] *See* Adam Shostack, *Threat Modeling, What, Why, and How*, Shostack + Associates (June 12, 2017), https://shostack.org/resources/whitepapers/threat-modeling-what-why-how.

[14] Gus Andrews, *User Personas for Privacy and Security*, Gus Andrews (Apr. 4, 2015), https://gusandrews.medium.com/user-personas-for-privacy-and-security-a8b35ae5a63b.

as information about medical, cultural, political, sexual, religious or other sensitive topics, while protecting their privacy with respect to these subjects.[15] These users may seek to bypass different forms of censorship while maintaining a separation between different social spheres or aspects of their identity.[16] Still other users seek mainly to avoid consumer threats such as spam, advertising-related malware, and identity theft, while delegating security-related decisions to vendors like Apple and accepting the limits on functionality they impose. Such users may be particularly vulnerable to "'social engineering' techniques to trick the user into granting access." *See* 1-ER-109.

The district court's findings show that Apple's policies primarily serve this last category of users. The court noted that Apple rejects apps that it deems not "trustworthy," or containing "objectionable" content, even when such apps and their content and functionality are "affirmatively authorized by the user." 1-ER-108. The court also found that while Apple's security reviews are effective for many users, a competitive app market could serve a broader range of consumer demands for

[15] *See* Marta Belcher, *OnlyFans Content Creators are the latest Victims of Financial Censorship*, EFF Deeplinks Blog (Aug. 24, 2021), https://www.eff.org/deeplinks/2021/08/onlyfans-content-creators-are-latest-victims-financial-censorship; Peter Eckersley, *6 Ideas For Those Needing Defensive Technology to Protect Free Speech from Authoritarian Regimes*, EFF Deeplinks Blog (July 17, 2009), https://www.eff.org/wp/surveillance-self-defense-international.

[16] Andrews, *supra* note 14.

security if third-party payment processing and other currently forbidden functionality were allowed into the App Store. Competing payment processing providers may "better detect fraud" because they process more transactions than Apple. 1-ER-119. Competitors may also promote security by *reducing* the number of users whose data could potentially be at risk from a data breach. 1-ER-120 ("[A]lthough a breach of a payment handler could expose some user data, a breach of Apple itself could expose all Apple users who use [in-app payment]."). And "third-party app stores could also have increased security than Apple." 1-ER-110 n. 527.

Apple's policies actively thwart developers' attempts to meet other user needs relating to privacy, security, trustworthiness, and access to information. For example, in 2019, Apple "removed or restricted" many of the most-downloaded apps for limiting screen time.[17] Apple's built-in functions for limiting screen time lack many of the functions that the banned apps provided.[18] Apple has also removed apps that perform important security functions, such as an app that tells the user if their phone has been "jailbroken" (a disabling of Apple's security features), which could

[17] Jack Nicas, *Apple Cracks Down on Apps That Fight iPhone Addiction*, N.Y. Times (Apr. 27, 2019), https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html.

[18] *Id.*

indicate the presence of surreptitiously installed surveillance programs.[19] And Apple has removed podcast apps from its Chinese app store, apparently because the developers of those apps did not engage in censorship at the request of the Chinese government.[20]

The district court found that demand exists for apps that take different approaches to security, privacy, and content than Apple's policies allow, but "Apple actively denies [users] the choice." 1-ER-122. This shows that Apple's approach to security is not a procompetitive justification, but is itself anticompetitive.

B. Generalized Security Rationales for Anticompetitive Conduct Should Be Accorded No Weight Under the Rule of Reason.

Evaluating business practices against an overly broad definition of security risks mischaracterizing overtly anticompetitive practices as procompetitive. Operators of technological systems often argue that security and reliability, broadly defined, require severe limits on users' ability to connect third-party products and services to the system. For example, at the height of its monopoly control over telecommunications in the United States, AT&T argued that reliable operation of the

[19] Andy Boxall, *Apple has pulled an app that told you if your iPhone was hacked*, DigitalTrends (May 16, 2016), https://www.digitaltrends.com/mobile/system-and-security-info-iphone-app-news/.

[20] Rita Liao, *Pocket Casts and Castro Podcasts removed from Apple's China store,* TechCrunch (June 11, 2020), https://techcrunch.com/2020/06/11/pocket-castro-podcast-removed-from-china/.

telephone network required their "absolute control over the quality, installation, and maintenance of all parts of the system." *In the Matter of Use of the Carterfone Device in Message Toll Tel. Serv.*, 13 F.C.C. 2d 420, 424 (1968). AT&T therefore required all of its subscribers to use only AT&T's own phones. To "divide the responsibility for assuring that each part of the system is able to function effectively," argued AT&T, would inevitably degrade the value of the system. *Id.*

This monopolist's view of security is discredited, because experience has shown that presumptions about the impact on security and reliability of allowing a broader range of third-party technologies to connect with a system are unwarranted. In *Carterfone*, for example, the Federal Communications Commission ruled that where actual harm to the system had not been shown, AT&T could not apply a general presumption that third-party devices are harmful as a basis for banning the connection of such devices. *Id.*

In addition, putting responsibility for the security and reliability of a system in the hands of one entity risks exposing users to vulnerabilities that entity fails to address. For example, in 2016, Apple refused improper demands that it re-engineer the iPhone to give law enforcement greater access to users' stored communications, on the grounds that doing so would put all users' privacy at greater risk from

malicious actors.[21] But in 2020, Apple reversed course and proposed to add novel message-scanning technology to its devices as part of a law enforcement function, risking the same security and privacy threats the company had previously stood against.[22]

To be sure, this appeal does not involve a complete ban on third-party products and services such as the one challenged in *Carterfone*. But that decision, and the potential risks created by a "security monoculture," both counsel against treating as conclusive to rule of reason analysis a defendant's arguments that conflate selectiveness itself with security.

C. The Inconsistent Application of Apple's Policies and Their Opacity to Developers and Consumers Demonstrate that Apple's Security Rationale is Entitled to No Weight.

Another problem with Apple's invocation of security as a procompetitive rationale is the company's opaque, arbitrary, and byzantine enforcement of its app store policies. In 2020, Apple blocked an update of the email app HEY, including fixes for the app's security, and threatened to remove the app entirely, because the app and its associated service accepted subscription payments through the

[21] Rainey Reitman, *The Apple Fight is About All of Us*, EFF Deeplinks Blog (Mar. 17, 2016), https://www.eff.org/deeplinks/2016/03/apple-fight-about-all-us.

[22] Kurt Opsahl, *If You Build It, They Will Come: Apple Has Opened the Backdoor to Increased Surveillance and Censorship Around the World*, EFF Deeplinks Blog (Aug. 11, 2021), https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance.

developer's own website, rather than through Apple's proprietary in-app purchase system.[23] Yet Apple allows some of the most-used apps, including Netflix, Spotify, and Amazon Kindle, to collect sign-ups and subscription payments exclusively from channels outside of their apps, bypassing Apple's payment system and commissions entirely.[24] Over a year later, as part of a settlement with Japan's antitrust enforcement agency, Apple retroactively created an exception in its App Store rules for what it called "reader" apps, a category that includes the widely-used apps but not email clients like HEY.[25] Apple's justification for the rule change relies on a distinction between audiovisual content (digital magazines, e-books, movies, and audio) on one hand, and "digital goods" on the other—an arbitrary line with no clear security or other procompetitive rationale. A technology reporter described this shifting set of policies and their enforcement as "you have to use Apple's [payment] system unless you were lucky enough to make a popular subscription app, in which case you could

[23] Rainey Reitman, *Apple's Response to HEY Showcases What's Most Broken About the Apple App Store,* EFF Deeplinks Blog (June 22, 2020), https://www.eff.org/sh/deeplinks/2020/06/apples-response-hey-showcases-whats-most-broken-about-apple-app-store.

[24] Will Oremus, *Apple's Secret Monopoly*, OneZero (Feb. 25, 2020), https://onezero.medium.com/apples-secret-monopoly-5718272c16a5.

[25] Jon Swartz, *Apple loosens App Store payment rules for 'reader' apps in another concession to developers,* MarketWatch (Sept. 2, 2021), https://www.marketwatch.com/story/apple-loosens-app-store-payment-rules-for-reader-apps-in-another-concession-to-developers-11630552977.

just keep going."[26]

In another example of Apple's inconsistent application of its App Store policies, the company introduced a privacy-enhancing feature in 2020 that allows users to opt out of having their identity and activities tracked across multiple third-party apps.[27] But several of the largest app developers, including Facebook and Snap, continue to harvest device-identifying data from Apple devices that could be used for cross-app tracking. Apple is reportedly aware of this practice, and condones it, though it tells developers they must "anonymize" the data.[28]

The Supreme Court recently refused to give deference to a procompetitive rationale for which an antitrust defendant "had not offered any consistent definition," but instead had "shifted markedly over time." *Nat'l Collegiate Athletic Ass'n v. Alston*, 141 S. Ct. 2141, 2163 (2021). Just as the NCAA's restrictions on compensation for student athletes could not be justified based on an inconsistent definition of "amateurism," Apple's restrictive App Store rules cannot be justified

---

[26] Dieter Bohn, *Apple's App Store policies are bad, but its interpretation and enforcement are worse*, Verge (June 17, 2020), https://www.theverge.com/2020/6/17/21293813/apple-app-store-policies-hey-30-percent-developers-the-trial-by-franz-kafka.

[27] Chance Miller, *Report: Snap and Facebook use App Tracking Transparency loophole to continue sharing 'aggregated' user data*, 9To5Mac (Dec. 8, 2021), https://9to5mac.com/2021/12/08/snapchat-facebook-data-sharing-app-tracking-transparency/.

[28] *Id.*

by an inconsistent and selective approach to security. *Id.*

D. Epic's Proposed Alternative of a Notarization Model Offers Comparable Security Without Restricting Competition.

Having overstated the impact of Apple's security rationale, the district court drew the wrong conclusions from its finding concerning Epic's proposed alternative to Apple's exclusive control over app distribution.

The district court's conclusion that notarization is not a valid alternative to exclusive control over app distribution was inconsistent with the court's own findings of fact. In a notarization model, Apple would review apps and affix its digital signature to apps that pass its review. Apps could then be distributed through any channel, including but not limited to the App Store. The court credited Apple's assertion that a notarization model including human review of apps "would not scale well." 1-ER-151. But the court had found that notarization could entail *exactly the same* level of human and automated review that Apple currently gives to all apps it allows into the App Store. 1-ER-116. Notarization would simply make app review "independent of app distribution," a procompetitive outcome that the district court found would not decrease security. *Id.* ("[A]lternative models are readily achievable to attain the same ends even if not currently employed."). Given these findings, the court's conclusion that notarization of apps would be less effective or significantly more costly than Apple's current App Store policies makes no sense.

The district court considered the notarization approach that Apple uses for the

Mac platform, observing that, prior to Epic's lawsuit, "Apple has consistently represented Mac as secure and safe from malware." 1-ER-116. Notably, Apple adopted the Mac notarization model when it did not possess market power and "at a time when users expected to freely download [applications] from the Internet, which limited Apple's ability to impose greater restrictions given customer expectations." 1-ER-115. Yet the court rejected Apple's argument that the Mac platform was less secure. 1-ER-116.

This suggests that a notarization model, perhaps similar to the Mac model but with human review of apps, would also be accepted by consumers as an alternative to App Store exclusivity—an alternative that does not restrict competition. The existence of such an alternative demonstrates that, on balance, Apple's policies do not promote competition. *See Amex*, 138 S. Ct. at 2284 (If "the procompetitive efficiencies could be reasonably achieved through less anticompetitive means," then the challenged conduct is illegal under the rule of reason.).

CONCLUSION

A holistic review of the district court's factual findings will show that Apple does have market power in app distribution, and that its proffered justifications for its restrictive App Store policies do not outweigh the anticompetitive effects of those policies. Accordingly, this Court should find Apple's policies to be illegal under the Sherman Act. This result will leave Apple free to continue innovating for

the benefit of its users, while allowing innovation to flourish outside of Apple's walls as well.

Dated: January 27, 2022

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

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

Harrison McAvoy
Ankur Kapoor
CONSTANTINE CANNON LLP
335 Madison Avenue
9th Floor
New York, NY 10017

David Golden
CONSTANTINE CANNON LLP
1001 Pennsylvania Ave NW
Ste. 1300N
Washington, DC 20004

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 Appellant, Cross-Appellee Epic Games and Reversal with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,647 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 font in Times New Roman font.

Dated: January 27, 2022

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 27, 2022.

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 27, 2022

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

Counsel for Amicus Curiae