Nos. 21-16506 & 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/counter-claimant,
Appellee/cross-appellant.

On Appeal from the United States District Court
for the Northern District of California (Hon. Yvonne Gonzalez Rogers)
No. 4:20-cv-05640-YGR-TSH

BRIEF OF *AMICUS CURIAE* THE CENTER FOR CYBERSECURITY POLICY AND LAW IN SUPPORT OF APPELLEE/CROSS-APPELLANT

Marc J. Zwillinger
ZWILLGEN PLLC
1900 M Street, N.W.
Washington, DC 20036
(202) 296-3585

James Orenstein
ZWILLGEN PLLC
183 Madison Avenue, Suite 1504
New York, NY 10016
(646) 362-5590
orenstein@zwillgen.com

Attorneys for The Center for Cybersecurity Policy and Law

CORPORATE DISCLOSURE STATEMENT

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

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

Statute

Rule

Other Authorities

TABLE OF AUTHORITIES
(continued)

Page(s)

STATEMENT OF IDENTITY AND INTEREST OF *AMICUS CURIAE*[1]

The Center for Cybersecurity Policy and Law ("Center") is a nonprofit organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. Its interest in this case is to ensure that courts applying the Rule of Reason to cases arising in markets that flourish and depend on secure technology and robust privacy protections – which is virtually all markets in an increasingly interconnected world – give due consideration to the procompetitive effects of cybersecurity measures. As the district court recognized below, companies that take steps to ensure cybersecurity and privacy are promoting competition even as their embrace of such competitive differentiators advance their own interests and the interests of their customers. Such a recognition is essential to avoid creating perverse incentives that will stifle innovation, create security risks for consumers, and ultimately stunt the growth of otherwise competitive markets.

INTRODUCTION

A basic premise of the Rule of Reason is that procompetitive conduct is lawful, even if it also has a substantial anticompetitive effect, so long as there is no

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

viable alternative that is less restrictive. The district court, apparently without any objection at trial from Appellant/Cross-Appellee Epic Games, Inc. ("Epic"), understood that in undertaking such analysis, it could properly consider the efforts of Appellee/Cross-Appellant Apple Inc. ("Apple") to promote robust data security and privacy protections as procompetitive conduct. However, Epic and some of its supporting amici now argue not simply that the district court reached the wrong result below, but that it was legal error for the court even to consider the safety and privacy of digital ecosystems in its Rule of Reason analysis. They argue that no matter how beneficial such conduct may be in other ways, courts must ignore a company's efforts to ensure a safe market for the development and sale of mobile apps if it involves any reduction in customer choice because they contend that those efforts cannot be deemed to promote competition. *See* Opening Brief For Appellant, Cross-Appellee Epic Games, Inc. ("Epic Br.") at 52-53; Brief of *Amici Curiae* 38 Law, Economics, and Business Professors in Support of Appellant/Cross-Appellee ("Professors Br.") at 6-14.

The argument is both wrong and potentially dangerous. Accepting it (despite the fact that no party to the litigation endorsed it at trial) would likely undermine rather than support the kind of competition that creates greater security and privacy for users and leave consumers and organizations to largely fend for themselves in implementing and managing security and privacy in mobile ecosystems. It would

disincentivize innovations specifically designed to give consumers the confidence to buy and use mobile apps and preclude a type of product differentiation that benefits consumers and that they clearly value. *See* 1-ER-48 n.250 (noting that consumers, including Epic's founder, value Apple's privacy and data security measures). Even if consumers do not fully comprehend all the technical ways in which they benefit from these approaches, the fact that they can choose an ecosystem that maintains a safe and privacy-protective app store gives consumers confidence that that there is a safe way to download and use apps – some of which hold their most sensitive data. The Court should therefore reject the argument that security and privacy benefits cannot be considered procompetitive.

In rejecting Epic's federal antitrust claims, the district court made findings that precluded judgment in Epic's favor and obviated the need to analyze the challenged conduct of Apple under the Rule of Reason. Specifically, the court found that Epic did not prove the existence of the market it alleged or that Apple had monopoly power or engaged in concerted action. 1-ER-48, -49, -68, -145 to -146. The district court nevertheless, in the interest of completeness, considered the reasonableness of Apple's conduct. 1-ER-146. It found both that Apple had valid, non-pretextual justifications for that conduct and that Epic had failed to propose a viable, less restrictive alternative. 1-ER-148 to -152.

Epic contested the factual issues below but appears to have at least tacitly acknowledged that the district court's inquiry into all of Apple's proffered justifications for the challenged conduct – including its focus on security and privacy – was an appropriate part of the required legal analysis. *See* 1-ER-107 (summarizing Apple's proffered procompetitive justifications and describing Epic's response as "each of these justifications is pretextual").[2] Epic, with the support of a group of law professor amici (the "Professors"), takes a new and disturbing tack before this Court, raising an argument that prompts the Center's participation in this briefing. Distorting the holding and rationale of *National Society of Professional Engineers v. United States*, 435 U.S. 679 (1978) ("*Engineers*"), Epic and the Professors contend that creating a mobile app ecosystem that protects data security and privacy has nothing at all to do with competition.

That assertion – which ignores the consensus views of cybersecurity professionals not only in academia, but also those in civil society, commerce, and government – is wrong as a matter of fact and law and could have potentially

[2] As Apple has noted in its brief to this Court, Epic's acknowledgement that the district court could properly take the security justification into account was actually more than just tacit. *See* Principal and Response Brief for Appellee/Cross-Appellant Apple Inc. at 78 (quoting Epic's expert as conceding that "[p]rotecting iPhone users from security threats is a procompetitive benefit").

disastrous cybersecurity consequences, especially in a time when information security threats are at unprecedented levels.[3]

Mobile devices and their apps have become ubiquitous in our society in recent years. Consumers and businesses use devices and apps in every aspect of their existence – for productivity, commerce, healthcare, social networking, employment opportunities, entertainment, and more. As apps become a more pervasive part of our lives and our economy, establishing a secure and privacy-respecting mobile ecosystem is essential, and the methods for achieving security and privacy controls within that ecosystem must not be compromised in a way that increases risk to end users. Further, a safe mobile ecosystem is more than just an indispensable facet of the economy, it is an important part of why a vibrant, competitive market exists in the first place. The fact that some app stores have incorporated security and privacy into the basic structures of their systems has fostered a level of public trust in mobile apps that has made possible the explosive growth in mobile device and app usage to date. In addition, creating such secure and private mobile ecosystems is in itself way for the providers of app stores to differentiate themselves from – and thereby compete with – their rivals in the marketplace. For those reason, courts can and

[3] *See* Center for Cybersecurity Policy and Law, *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy* (May 2021), https://centerforcybersecuritypolicy.org/initiatives ("Mobile Future") at 7-8 (citing AV-Atlas Statistics, https://portal.av-atlas.org/malware/statistics).

should – as the district court did in this case – recognize that creating and maintaining a secure mobile ecosystem is procompetitive.

ARGUMENT

I. BUILDING SECURITY AND PRIVACY IS PRO-COMPETITIVE

Building security and privacy into the mobile ecosystem promotes, rather than hinders, competition. When the first mobile telephones became available decades ago, they were "dumb" devices, within the financial reach only of a relative few, that provided just one basic function: mobile audio communication. By 2007, mobile devices had become somewhat more affordable and offered a few more functions, but in that year, as the district court observed, Apple's iPhone innovation transformed the marketplace by

> creating a new and innovative ecosystem to break into the cellular device market with established competitors such as Samsung, Nokia, LG, Sony, Blackberry, Motorola, Windows Mobile, and Palm. No one disputes that the iPhone was revolutionary and fundamentally changed the cellular device market. Given the years that have passed, one may forget how fundamentally different the iPhone was to the alternatives.… The device offered users the ability to access email, browse the web, and perform certain software applications by simply tapping a square-ish icon on the screen called an "app," short for a software application.

1-ER-30.

The advent of the iPhone and other smartphones has sparked a massive increase in use: these connected, multifunctional mobile devices have become a basic part of life for billions of people and their businesses across the globe, and

their reach and sophistication continue to grow. Recent estimates have suggested that there are more than 5.50 billion unique mobile subscribers globally, up from just over 4.00 billion at the start of 2015. This includes the estimated 3.78 billion individuals, nearly half the world's population, that were classified as mobile internet users by the end of 2019, an increase of roughly 250 million from the previous year.[4] These mobile device users are increasingly relying on smartphones. The uptake in smartphone devices, while comprising a higher total in more traditionally developed international regions, has seen tremendous growth in all regions over just the past few years. Globally, the estimated share of smartphones as a percentage of mobile connections has risen from just over 30 percent in 2014, to just under 70 percent by 2019.[5] This growth has, in large part, happened because of, not in spite of, the increased security and privacy provided by mobile devices over desktop and personal computers, especially with iOS-based devices.

As more people use more sophisticated devices, they use them for a wider range of activities. While this case involves only one part of the digital world – the

---

[4] *See* Mobile Future at 4-5 (citing Ericsson Mobility Report (Nov. 2020), https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf ("Ericsson Report")).

[5] *See generally* Mobile Future at 4-5 (citing GSMA, *The State of Mobile Internet Connectivity 2020*, https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf) ("GSMA Report")).

district court found that "the relevant market here is ***digital mobile gaming transactions***," 1-ER-4 (emphasis in original) – this Court's decision about whether to recognize the procompetitive effect of secure mobile ecosystems will have a far broader impact on the way the world uses mobile devices. No longer just a means of audio communication, people and businesses use mobile devices to access news and government services, manage their banking and finance, pay for goods and services, track illnesses and disseminate other healthcare information, and look for and fill job openings.

These increasingly sophisticated, more sensitive uses are possible in part because of the growth in mobile apps and the app stores that distribute them and made further possible by the security that is provided to consumers by app stores that carefully vet apps so that the consumer need not discern for herself which apps are safe to use, and which pose a serious threat. What started as a few hundred apps now number in the millions. *See* 1-ER-39; Mobile Future at 5. Millions of developers work to build those apps; and mobile device users download tens of billions of them each year. *See* 1-ER-32; Mobile Future at 5.

Those millions of apps are available in many different app stores. Just within the mobile game app sector, as the district court recounted, the number of marketplace participants has grown since Apple launched the App Store in 2008, with Google announcing what is now Google Play the same year, and Nokia,

Samsung, and Nintendo launching their own app stores soon after. 1-ER-75. As of 2020, there were over 300 app stores worldwide, and that number continues to grow.[6]

Most app stores, regardless of mobile platform or owner, have a similar functionality and aesthetic that end users have come to recognize and expect. Finding and installing a desired app is practically seamless. But the apps themselves can vary widely in terms not only of quality but also safety and privacy. Likewise, the sources of these apps are far from equal – particularly with respect to the security and privacy protections they provide. Those differences can dramatically affect the risk to mobile app users: for example, most malware is distributed from sources that do not perform comprehensive checks of applications they provide.[7]

The riskiest model by far for uninformed end users is sideloading, which involves installing an app onto a mobile device outside the context of an app store, such as by downloading the app from a web site and installing it directly. *See* 1-ER-21 & n.124. Different mobile platforms take different approaches to sideloading. For

---

[6] See Mobile Future at 5 (citing Wandera, *Understanding the Key Trends in Mobile Enterprise Security in 2020*, https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf ("Wandera Report")).

[7] *See* Mobile Future at 6 (citing CrowdStrike, Mobile Threat Landscape Report 2019, https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/).

example, some versions of Android OS make sideloading relatively simple: users can affirmatively choose to enable the function with minimal effort, even if it is initially off by default. Apple has no such setting to easily enable sideloading – and for good reason. As Apple and the security and privacy experts convened by the Center both recognize that sideloading presents perhaps the greatest risks to users – it removes any platform-based curation around privacy and security, placing a significant security burden on the user to determine if the sideloaded software is safe, secure, and authentic. The more common sideloading becomes, the harder it will be for a consumer to differentiate between "safe" and "unsafe" apps.

Almost as risky to uninformed users are completely un-curated app stores, which essentially serve as conduits for indirect sideloading. As with direct sideloading, end users still must enable the app store to be accessible on their device – but once they do so, they can download any app regardless of risk, and app developers can thereby release products directly to consumers with no scrutiny by the app platform. This model places all the burdens on the consumer to protect themselves – a task that most consumers cannot be expected to perform effectively, and certainly not at scale. *See* 1-ER-109; Mobile Future at 7-8. And it makes the consumer the last line of security defense against malicious actors, who can leverage the user's lack of security experience and the inherent trust that they have established in the platform.

On the other end of the spectrum is the fully curated app store where the owner constructs an ecosystem that tightly integrates the hardware, operating systems, apps, and even payment systems. While no model can completely keep malicious or fraudulent apps from reaching end users, this fully curated approach dramatically reduces risk and removes much of the security burden from the consumer.

Apple's App Store ("App Store") is the paradigmatic fully curated ecosystem. As the district court noted, its guidelines preclude authorization of malicious and privacy-invasive apps, among others. 1-ER-39; *see also* 1-ER-40 ("Apple proactively requires, much to some developers' chagrin, measures to protect data security, privacy, data collection and storage. The data collection and disclosure requirements are not insignificant.") (footnote omitted); 1-ER-42 (Apple's guidelines "place the customer's concerns ahead of the developers and are on the forefront of protecting user data; measures not all developers embrace, especially where they want to monetize that data."). Apple employs a variety of methods to protect against malware, including automated scanning for known malware programs, developer authentication requirements that allow malware to be traced and code from unrecognized sources to be blocked, technical barriers that prevent

apps from acting in ways the user has not authorized, and automated and human reliability checks. 1-ER-108.[8]

As the district court found, this fully curated approach is effective, producing a "relatively small" error rate. 1-ER-110. Critically, the district court made the further factual finding that the App Store's effectiveness in creating a safe ecosystem depends on the ways in which it restricts the distribution of unvetted apps:

> Removing app distribution restrictions could reduce this effectiveness [in providing security against malware]. First, app stores often differ in the quality of app review. On Android, which allows some third-party app stores, the main Google Play app store is secure, but a variety of third-party stores allow blacklisted apps to operate. A Nokia report attributes higher malware rates on Android to Trojan apps on third-party app stores. This creates a problem because, as Dr. Rubin opined, "security is only as strong as the weakest link." Decentralized distribution thus increases the risk of infection by giving malware more opportunities to break through. Namely, if even one app store permits malware to operate (either accidentally or as a "rogue" app store), a social engineering attack has a chance to work.
>
> Second, with respect to sideloading, app review is likely impossible and thus could not prevent social engineering attacks. Apple currently prevents direct distribution from the web using technical measures. If those measures were lifted, users could download—and thus could be tricked into downloading—directly from the open web. Although Epic Games presents some alternative methods that could be used to prevent malicious direct distribution … there is little dispute that completely unrestricted sideloading would increase malware infections.

[8] This multi-layered approach is effective because different review methods can be more or less successful in preventing different types of harm. Thus, for example, research has demonstrated that automated scanning is particularly effective in reducing known malicious apps, but that human review is an essential component of combating fraudulent apps. *See* Mobile Future at 9-10.

> Thus, the Court finds that centralized distribution through the App Store increases security in the "narrow" sense, primarily by thwarting social engineering attacks.

1-ER-110 to -11 (footnotes omitted). Likewise, the district court found as a matter of fact (in part because there was "less dispute" about it) that largely because of its reliance on human review, Apple's "app distribution restrictions help ensure privacy, quality, and trustworthiness." 1-ER-111.

The protections afforded by a fully curated app store are particularly beneficial – and also procompetitive – because many users lack the technical sophistication needed to make informed security decisions. The district court's finding that a curated app store helps prevent users from being tricked into downloading malicious apps is well-founded. Mobile platforms are susceptible to many types of malware, and both non-state criminal actors and nation-state actors waste little time in developing new malware or adapting existing malware to the mobile environment.[9] Similar challenges exist with respect to digital privacy: many users lack the time and expertise to gain a clear understanding of how an app might use – or misuse – their personal data, even if the app provides a transparent account on that score.[10]

---

[9] *See* Mobile Future at 7 (citing CrowdStrike, Mobile Threat Landscape Report 2019, https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/).

[10] *See* Mobile Future at 8 (citing Brooke Auxier and Lee Rainie, *Key takeaways on Americans' views about privacy, surveillance and data-sharing*, Pew Research

Given the extent and complexity of the risk, leaving users to fend for themselves in the market for apps is unrealistic and unsafe. More pertinently, it also undermines competition. A competitive market may not need ***all*** app stores to create mobile ecosystems that protect security and privacy, but if ***no*** mobile ecosystem or app store does so, consumers who value those interests could lose confidence that there is a safe way to download and use apps, especially for sensitive functions.

The resulting loss of system confidence would reduce output and harm all concerned – users, developers, and app store platforms. As the district court found after reviewing the evidence at trial below, "many users value their iOS devices for their privacy and security. As the result of having a trusted app environment, users make greater use of their devices, including by storing sensitive data and downloading new apps. The witnesses are unanimous that user security and privacy are valid procompetitive justifications." 1-ER-114. Likewise, the district court found that "developers benefit from the safe environment created by the App Store. Based on a trusted environment, users download apps freely and without care, which benefits small and new developers whose apps might not be downloaded if users felt concern about safety." 1-ER-114. Further, because some users care more about security and privacy than others – and because some users are undoubtedly better

---

Center (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/).

equipped than others to protect themselves without relying on an app store's curation – the distribution constraints that are necessarily part of a curated app store are themselves a form of product differentiation that promote competition among different app stores – a reality again reflected in the district court's factual findings. *See* 1-ER-113 (finding that since the App Store's launch, "security and privacy have remained a competitive differentiator for Apple").

The district court's detailed factual findings below thus confirm the consensus view of cybersecurity experts from the private sector, civil society, and government: curated app stores like Apple's create mobile ecosystems that enhance user security and privacy and thereby allow competition to flourish. Contrarily, a legal regime that disincentivizes such a focus on safety could have a pernicious effect – not only on the users who would more readily fall victim to malware, fraud, and invasions of privacy, but also on the developers whose success depends on users' trust. Federal antitrust law creates no such disincentive, as the district court properly recognized and as discussed below.

II. A COURT APPLYING THE RULE OF REASON IS CLEARLY ALLOWED TO FIND THAT PROTECTING SECURITY AND PRIVACY CAN BE PROCOMPETITIVE

Controlling law clearly permits a court to recognize the procompetitive aspects of protecting security and privacy, as the district court did. Epic's argument that the district court committed legal error simply by considering the possibility that

Apple's security measures are procompetitive has no support in the briefs or the law – nor should it. As support for its assertion that the court committed "error," it invokes a selective and misleading quotation from *Engineers*, and an inapposite quotation from another case. *See* Epic Br. at 53 (quoting *Engineers*, 435 U.S. at 695; *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 463 (1986) ("*Dentists*")). The Professors make the bolder claim that the district court committed "fundamental" error because it "accepted business rationales that … are, as a matter of law, not cognizable antitrust justifications." Professors Br. at 2; *see id*. at 6-14. As explained below, neither Epic nor the Professors accurately describe or apply controlling law on this point.[11]

[11] Because the Center's interest in this case focuses exclusively on the critical importance of acknowledging the procompetitive effect of maintaining a safe mobile ecosystem, and the propriety of doing so as part of the Rule of Reason inquiry, this brief generally does not address other potential areas of disagreement with the parties or other amici. However, it advances the Center's interest to note that the Court should reject Epic's argument about ignoring the procompetitive justification for a curated app store for the independent reason that the district court found that Epic's claim failed at the first step of the Rule of Reason inquiry. Both Epic and the Professors contend that the district court found that Apple's distribution restrictions have "substantial anticompetitive effects." Epic Br. at 13; Professors Br. at 5. That is incorrect. While the court stated that Apple's distribution restrictions had "some" anticompetitive effects, 1-ER-147, that finding falls short of what is needed to clear the first hurdle of the Rule of Reason analysis and establish liability. *See*, *e.g.*, *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2284 (2018) (plaintiff's "initial burden [is] to prove that the challenged restraint has a substantial anticompetitive effect").

At the heart of the legal discussion of the issue in both briefs is the Supreme Court's decision in *Engineers*. Epic Br. at 53; Professors Br. at 8-9. But the facts of that case are not comparable to those here, and the Supreme Court did not in any event create the inflexible – and inherently ***unreasonable*** – exception to the Rule of Reason that Epic and the Professors propose.

Unlike the dispute in this case, *Engineers* involved an explicit ban on competition as such. The National Society of Professional Engineers ("Society") had adopted a "Code of Ethics" that forbade members from submitting competitive pricing bids for their engineering services, so as to preserve a tradition of having clients select engineers on the basis of background and reputation rather than price. 435 U.S. at 684. When the government sought an injunction barring that "ethics" rule on the ground that it suppressed competition, the Society pleaded a series of affirmative defenses, only one of which remained by the time the case reached the Supreme Court: they argued that "the standard set out in the Code of Ethics was reasonable because competition among professional engineers was contrary to the public interest." *Id*. The Supreme Court unsurprisingly rejected the Society's sophistry.

The Court began its analysis by summarizing its earlier decision in *Goldfarb v. Virginia State Bar,* 421 U.S. 773 (1975), holding that a minimum fee schedule for legal services violated Section 1 of the Sherman Act, 15 U.S.C. § 1. As the Court

acknowledged at the outset, *Goldfarb* "noted that certain practices by members of a learned profession might survive scrutiny under the Rule of Reason even though they would be viewed as a violation of the Sherman Act in another context." *Engineers*, 435 U.S. at 686. Moving on to address the Rule of Reason itself, the Court noted that some interpretive rule is needed because the Sherman Act, the text of which prohibits "every" contract that restrains trade – which necessarily encompasses every commercial contract – "cannot mean what it says." *Id*. at 687 (citing *Chicago Bd. of Trade v. United States*, 246 U.S. 231, 238 (1918)). That interpretive guide is the Rule of Reason, which "has been used to give the Act both flexibility and definition …. [and] focuses directly on the challenged restraint's impact on competitive conditions." *Id*. at 688.

Epic and the Professors construe *Engineers* to foreclose inquiry into any proffered justification for a substantial competitive restraint that is predicated on security and privacy. *See* Epic Br. at 53 ("To the extent [the district court] credited [Apple's security and privacy justifications] at all, that was error."); Professors Br. at 6 ("The court erred as a matter of law in treating what it called the 'security, privacy, and reliability' benefits claimed by Apple as cognizable justifications[.]"). But that interpretation misses the mark in a fundamental way: *Engineers* disallows "benevolent dictator" rules that arrogate to a defendant the decision that society should let competition take a back seat to some other value, but it does not prevent

a court from finding that a restraint of trade motivated by some other value such as privacy can itself advance competition. What the Court wrote in *Engineers* is that its earlier decisions "foreclose the argument that because of the special characteristics of a particular industry, monopolistic arrangements will better promote trade and commerce ***than competition***." *Engineers*, 435 U.S. at 689 (citing *United States v. Trans-Missouri Freight Ass'n,* 166 U.S. 290 (1897) (emphasis added); *United States v. Joint Traffic Ass'n,* 171 U.S. 505, 573-577 (1898)).

Unlike *Engineers*, this is not a case where a defendant's policy furthers other, non-competition objectives as a ***substitute*** for competition altogether. *Cf. Engineers*, 435 U.S. at 684 (noting the Society's argument that "competition" itself "was contrary to the public interest"); *id*. at 695 (noting the Society justified the challenged rule "on the basis of the potential threat that competition poses"). It is that attempt to substitute a defendant's interest in other values for the Congressional decision to protect competition that the Court described as "nothing less than a frontal assault on the basic policy of the Sherman Act." *Id*. But that does not remotely mean that promoting public safety or any other non-monetary value can never be considered a ***procompetitive*** justification for a restraint of trade. By arguing to the contrary, Epic and the Professors mistake the Court's fundamental concern in *Engineers*: as the Court itself wrote, "[t]he true test of legality is whether the restraint imposed is such as merely regulates ***and perhaps thereby promotes competition*** or

whether it is such as may suppress or even destroy competition." *Id*. at 691 (emphasis added) (quoting *Continental T.V., Inc. v. GTE Sylvania, Inc*., 433 U.S. 36, 49 n.15 (1977) (quoting *Chicago Bd. of Trade*, 246 U.S. at 238)).

Here, Apple did not argue, and the district court did not find, that its app distribution rules are permissible because they promote free-standing societal interests in security and privacy; instead, the proffered (and accepted) justification was that, in the context of the relevant market for digital mobile gaming transactions, enhancing the security and privacy of a mobile app ecosystem is itself conducive to ***competition*** in that market. Thus, even if *Engineers* supported the rule that Epic and the Professors invent (which it does not), it would not undermine the lawfulness of the district court's sound factual finding that ensuring safety and privacy in mobile app ecosystems is itself procompetitive.[12]

[12] Epic and the Professors fare no better in attempting to rely on other cases, all of which they explicitly argue draw their authority from *Engineers* – which, as demonstrated above, does not support their position. *See* Professors Br. at 9-10 (citing the application of *Engineers* in the Court's *Dentists* opinion to an attempt by dentists to defend their "professional independence" by refusing to submit x-rays to insurers for use in benefit determinations); *id*. at 10 (citing *FTC v. Superior Court Trial Lawyers Ass'n*, 493 U.S. 411, 414 (1990), and its reliance on *Engineers* to find that a group of lawyers violated the Sherman Act by agreeing not to represent indigent defendants until the local government increased their compensation because they contended that raising their rates would improve the quality of their work); *id*. at 10-11 (citing *NCAA v. Alston*, 141 S. Ct. 2141, 2159 (2021), and its citation to *Engineers* to reject the NCAA request for "a sort of judicially ordained immunity from the terms of the Sherman Act for its restraints of trade . . . because they happen to fall at the intersection of higher education, sports, and money").

As with their misconstruction of *Engineers* itself, the Professors mischaracterize the argument that Apple made and that the district court accepted below. In their incorrect view, Apple is arguing that "interbrand competition—in this case, in robust app distribution—will lead to inferior product quality and that it should be therefore permitted to prohibit such competition." Professors Br. at 11. But what Apple actually argued, and what the district court actually found as a matter of fact, that its security and privacy protections ***promote*** competition, even if they have "some" insubstantial effects that otherwise restrain it.[13] By making that finding, the district court engaged in precisely the kind of analysis that is perfectly lawful under the Rule of Reason. *See* Professors Br. at 12. n.5 (acknowledging in a footnote that "Courts have accepted defendants' antitrust justifications only when they enhance competition.") (citing *Broadcast Music, Inc. v. CBS, Inc.*, 441 U.S. 1, 21–22 (1979) (joint selling arrangement created a new product that increased output and competition); *Continental T.V., Inc.*, 433 U.S. at 54 (restrictions on intrabrand competition ameliorated free-rider problems and other market failures and thereby "promote[d] interbrand competition")).

[13] In the Professors' view, the argument that promoting security and privacy in the mobile app ecosystem is cognizably procompetitive "is foreclosed as a matter of law." In support of this putative "matter of law," however, they do not cite any statute or judicial decision; instead, they cite an article – by a legal academic who did ***not*** join their brief. *See* Professors Br. at 11 & n.6 (citing Erika M. Douglas, *Data Privacy Protection as a Procompetitive Justification*, 36 Antitrust 1, 12 (Dec. 2021).

Finally, in making their incorrect argument, Epic and the Professors disagree not only with the district court and Apple, but also with one of Epic's own (otherwise) supporting amici. The Electronic Frontier Foundation ("EFF") challenges the district court's *factual* findings about the procompetitive effects of Apple's security measures but not the legal basis for weighing such arguments. To the contrary, EFF properly acknowledges that security measures can "support a rule-of-reason defense if they are in ***fact*** procompetitive." Brief of Amicus Curiae the Electronic Frontier Foundation in Support of Appellant, Cross-Appellee Epic Games and Reversal ("EFF Br.") at 14 (emphasis added); *see also id*. ("'Security' means different things for different market participants, and these differences are key to evaluating whether a security rationale is in ***fact*** procompetitive.") (emphasis added). Indeed, EFF quotes *Engineers* itself, and even highlights the critical word that defeats Epic's argument: "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.'" *Id*. (quoting *Engineers*, 435 U.S. at 695) (emphasis added by EFF).[14]

[14] In its amicus brief, the United States says nothing to support Epic's position that security and privacy cannot be considered procompetitive as a matter of law. *See* Brief for the United States of America as Amicus Curiae in Support of Neither Party at 15-20. To the contrary, the government's emphasis on weighing pro- and anti-competitive factors supports considering *all* such arguments rather than artificially

CONCLUSION

As mobile devices and the apps that run on them become ever more integrated into our daily lives, the measures that app store platforms take to ensure security and privacy become increasingly valuable. Creating safe and private mobile ecosystems is procompetitive in two fundamental ways: it encourages users and developers to more safely participate in a vibrant market and increase output, and it allows app store providers an opportunity to compete against one another based on quality of the protections they offer. Robust competition does not necessarily depend on every app store providing a minimum level of security and privacy protection, but it would likely suffer if there was no app store available to satisfy the concerns of consumer who value security and privacy. The district court therefore correctly applied the Rule of Reason by considering the security and safety justifications for Apple's app distribution rules and by making the factual finding that those rules are procompetitive. This Court should therefore affirm that portion of the district court's ruling.

Dated: March 31, 2022

Respectfully submitted,

s/ *James Orenstein*
James Orenstein

placing some out of bounds. The government cites *Engineers* only for the point that the decision requires a court to inquire "whether the challenged agreement is one that promotes competition or one that suppresses competition[.]" *Id*. at 17 (quoting *Engineers*, 435 U.S. at 691).

Marc J. Zwillinger
ZWILLGEN PLLC
1900 M Street, N.W.
Washington, DC 20036
(202) 296-3585

James Orenstein
ZWILLGEN PLLC
183 Madison Avenue, Suite 1504
New York, NY 10016
(646) 362-5590
orenstein@zwillgen.com

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) Nos. 21-16506 & 21-16695

I am the attorney or self-represented party.

This brief contains 5,729 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

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

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ James Orenstein **Date** March 31, 2022

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I certify that on March 31, 2022, 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.

All participants in the case are registered CM/ECF users and service will be accomplished by the appellate CM/ECF system.

Dated: March 31, 2022

s/ *James Orenstein*
James Orenstein