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 (No. 20-cv-05640-YGR-TSH)
The Honorable Yvonne Gonzalez Rogers

BRIEF OF *AMICI CURIAE* FORMER NATIONAL SECURITY OFFICIALS AND SCHOLARS IN SUPPORT OF APPELLEE/CROSS-APPELLANT

Roy T. Englert, Jr.
Leslie C. Esbrook
ROBBINS, RUSSELL, ENGLERT, ORSECK, & UNTEREINER LLP
2000 K Street NW, 4th Floor
Washington, D.C. 20006
Tel.: (202) 775-4500
renglert@robbinsrussell.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

Amici are a group of former officials and scholars with decades of experience in cybersecurity, national security, and intelligence practices. They have served at senior levels for Presidents of both parties and played an outsized role in the creation of modern national security law and policy. Collectively and individually, they have devoted decades to protecting U.S. national security and ensuring that cybersecurity threats are minimized to the greatest extent possible consistent with the laws of the United States. *Amici* write to offer the Court their informed perspective on the national security disruptions that would result if this Court required Apple to allow sideloading of third-party applications on its mobile operating platform.

INTRODUCTION AND SUMMARY

The United States is vulnerable to cyber intrusions from foreign adversaries. Specifically, mobile devices represent a key vector of cyber interference. Appellant and its *amici* seek a world in which more than half the mobile devices currently used in the United States would be forced to downgrade their security-protection features related to downloaded device applications, depriving consumers of the option to choose the iPhone's current security profile. That proposed change creates weighty

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

national security issues. *Amici* are not antitrust experts, but as security experts they can shed light on the ramifications of Epic's approach for national security, cybersecurity, and the public interest.

The ubiquity of mobile devices presents both large-scale gains and risks for society. The ease, immediacy, and volume of offerings on mobile devices has indisputably been a boon for most Americans, and the capabilities of these devices are increasing at a near-exponential rate. But with society's reliance on mobile devices comes the necessity to ensure that those tools are not exploited by our Nation's adversaries.

The district court's ruling, although not grounded in rationales of national security per se, offers the highest and best outcome for protecting the Nation from mobile-based cybersecurity threats. Those cybersecurity threats are all too real. They have become the preferred tool of state and non-state actors, perpetrated in creative and complex ways from malware to ransomware and Internet-of-Things attacks. Cybersecurity issues have been known since the early days of personal computing. Yet only in the last decade have the public and private sectors invested serious resources in protecting against cyber threats as the devastating consequences of those threats have become recognized as near-term likelihoods.

If Epic were to prevail, consumers, and the country, would be worse off. By eliminating interbrand competition on security, Epic would deprive consumers of

the ability to choose greater device security and protection. Epic would require the courts to step in as regulators to determine the appropriate level of app review security, a role that is anathema to antitrust law and national security priorities. And by requiring app stores to conform to the lowest-common-denominator of security protection, Epic would increase the risk of cyber intrusions because millions of phone users could download apps that had not been vetted through a multi-layer review process. Epic's counterfactual world would also curb innovation in device security features and create a monoculture approach to security that would leave millions of devices vulnerable to the same type of attack. These consequences are significant headwinds for our Nation's cybersecurity policy.

I. MOBILE DEVICES PRESENT KEY AREAS OF CONCERN FOR NATIONAL SECURITY

To understand why requiring Apple to change its security features so that consumers cannot choose devices running Apple's security ecosystem harms national security, we must understand the import of mobile threats.[2] Mobile devices have become an increasingly fundamental part of our lives. As the Chief Justice wrote for the Court in *Carpenter v. United States*, mobile devices "and the services they provide are such a pervasive and insistent part of daily life that carrying one is

[2] This brief focuses on application-based and mobile risks because they are germane to the case at bar, but these platforms are but two means of propagating cyber intrusions.

indispensable to participation in modern society." 138 S. Ct. 2206, 2220 (2018) (internal quotation marks omitted). Smartphone ownership has more than doubled in the United States over the last decade (from 35% to 85%), and nearly half of all Internet usage in the U.S. is from mobile devices, up nearly 10% in just four years.[3]

Naturally, then, mobile devices are increasingly becoming targets for bad actors to exploit (as both Apple's expert and Senior VP of Software Engineering explained to the district court).[4] China, Russia, Iran, and North Korea have made cyberattacks a top tool of their statecraft. With increasingly sophisticated methods, they, and other foreign adversaries, target mobile devices as the means of propagating cyber intrusions. Because of these increasing threats, cybersecurity has become a key priority of the public and private sectors in recent years. Thus, the implications of mobile cyber intrusions make security considerations of Apple's App Store of paramount importance for everyone.

---

[3] Chris Kolmar, *U.S. Smartphone Industry Statistics [2022]*, ZIPPIA (Jan. 30, 2022), https://perma.cc/TU2W-L2JY.

[4] *See* Trial Tr. 3362-65 (Federighi) ("iPhones are very attractive targets. . . . [B]ecause [they are] always with you, if someone wanted to track your location, if someone wanted to have a live mic on you to capture your conversations, if they wanted to get access to certain kinds of credentials and tokens you use to access maybe work systems, those are likely to be on your iOS device . . . ."); Dkt. 742-5 ¶ 23 (Rubin) (mobile devices are "faced with an extraordinary threat model" due to their portability and function as repository for sensitive personal and financial information).

A. Cyberconflict Has Become A Preferred Tool Of Our Nation's Adversaries.

National security threats to mobile devices are not limited to a unique subset of bad actors. The Director of National Intelligence has reported that in 2007 only two to three countries in the world possessed cyberattack capabilities, but by 2017 that number had grown precipitously to more than thirty countries.[5] Apple's expert explained to the district court this very phenomenon—that sophisticated attackers are often "directed and supported by established nation-states" and use "malicious apps to target high-profile victims and cause long-term damage on critical assets."[6] The broad scope of foreign adversaries in cyberspace makes mobile device security critical.

Examples of recent cyber intrusions as statecraft abound. Russia has used malware in Android apps for espionage and surveillance operations, collecting mobile device users' passwords, recording calls, and eavesdropping through infected phones' microphones.[7] It has also used adversarial cyber operations to destabilize U.S. elections, "hack[ing] into state and local computer networks in breaches that could allow Moscow broader access to American voting infrastructure" to instill

---

[5] Daniel R. Coats, Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community, at 5 (Feb. 13, 2018).

[6] Dkt. 742-5 ¶ 24 (Rubin).

[7] Thomas Brewster, *Fake PornHub and Google Android Apps Are Actually 'Russian Spy Tools'*, FORBES (July 24, 2019), https://bit.ly/369UnLH.

mistrust in the electoral system (a "perception hack")[8] or, in some cases, actually "delete or alter voter data."[9]

China has used its cyber capabilities to steal valuable trade secrets and commit intellectual property theft.[10] According to the former Director of Information Assurance at the National Security Agency (NSA), China's "theft of intellectual property robs the U.S. of decades of advancement that can't easily, or perhaps ever, be recovered."[11] China has also hacked the Office of Personnel Management to steal personnel data of U.S. government employees applying for security clearances.[12]

Iran and North Korea present similar threats. In 2019 alone, Iran conducted or researched attacks on financial institutions, critical infrastructure like pipelines and dams, government agencies, and universities with valuable intellectual property,

---

[8] Julian E. Barnes et al., *Russia Poses a Bigger Election Threat Than Iran, Many U.S. Officials Say*, N.Y. TIMES (Oct. 22, 2020), https://perma.cc/MKG3-SGCL.

[9] Michael Riley & Jordan Robertson, *Russian Hacks on U.S. Voting System Wider Than Previously Known*, BLOOMBERG (June 13, 2017), https://perma.cc/R32H-AQDE.

[10] Paul Park, *Experts Examine Asia's Approach to Cybersecurity*, BROOKINGS (Aug. 28, 2018), https://perma.cc/FPP6-CTLZ.

[11] Joseph Marks, *Is Russia or China the Biggest Cyber Threat? Experts Are Split*, WASH. POST (Jan. 20, 2022), https://perma.cc/Q6BQ-MRJF.

[12] Ellen Nakashima, *Chinese Breach Data of 4 million Federal Workers*, WASH. POST (June 4, 2015), https://perma.cc/LQ6Z-5XL7.

to name just a few.[13] North Korea, too, has used cyberattacks to "steal classified military secrets, abscond[] with billions of dollars in money and cybercurrency, h[o]ld computer systems hostage, and inflict[] extensive damage on computer networks."[14] Beyond these most egregious states, plenty of additional state and non-state actors perpetrate threatening cyber intrusions, too.[15]

Many of these cyber intrusions to date have occurred on networks, computers, or whatever technology platform has exposed and easily exploitable vulnerabilities. It is a testament to the robust security protections currently offered on mobile devices

---

[13] Center for Strategic & Int'l Stud., *Publicly Reported Iranian Cyber Actions in 2019*, https://perma.cc/D6SU-DBBR (last visited Mar. 31, 2022).

[14] Bruce Klingner, *North Korean Cyberattacks: A Dangerous and Evolving Threat*, THE HERITAGE FOUNDATION, Summary (Sept. 2, 2021); *see* Thomas Brewster, *North Korean Hackers Are Spreading Spyware on Google Play and Targeting Defectors Via Facebook*, FORBES (May 17, 2018), https://perma.cc/B6EN-6XGE (describing North Korean hackers "pilfering private data from infected phones"). *Cf.* Dan Goodin, *North Korean Hackers Unleashed Chrome 0-Day Exploit on Hundreds of US Targets*, ARS TECHNICA (Mar. 24, 2022), https://perma.cc/GSL6-RDB6 (describing recent malware attack on financial services and cryptocurrency platforms).

[15] For example, non-state actors may be sponsored by foreign states, independent terrorist organizations (foreign or domestic), or transnational criminal organizations, engaging in the same types of adversarial operations as state actors. They may act for personal financial gains, *see Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*, 2019 Public-Private Analytic Exchange Program, U.S. Dep't of Homeland Sec., at 2 (2019), or personal vendettas, such as pro-ISIS sympathizers exposing the names and locations of U.S. military servicemen in response to U.S. military action, *see* Mark Pomerleau, *State vs. Non-State Hackers: Different Tactics, Equal Threat?*, DEFENSE SYSTEMS (Aug. 17, 2015), https://perma.cc/KN4Y-GJTL.

such as the iPhone that massive state-based cyber intrusions have, for the most part, not occurred through mobile-based exploits. As foreign adversaries improve their threat capabilities, however, the risks to mobile devices will grow. If Epic were to prevail, mobile devices would immediately be subject to increased vulnerabilities for foreign adversaries to exploit. In short, mobile device security like that built into Apple's App Store currently serves as a frontline of our Nation's defense.

B. App-Based National Security Threats In Particular Are Becoming More Sophisticated And Creative.

As with mobile device growth, the "sheer number of apps available . . . has exploded" in the past decade.[16] App-based cyber intrusions propagated through malware, or malicious software, now represent a key vector of foreign interference. Though malware has been around since the early days of personal computing,[17] since 2010 the prevalence of devices and the investment of foreign adversaries into cyber capabilities has coalesced to create a "significant evolution in the sophistication of malware" in the national security arena. *Id.* Indeed, the FBI Director has compared the scale and challenges of device-based threats to the threat of 9/11, stating that "[t]here's a shared responsibility, not just across government agencies but across the

[16] U.S. Dep't of Homeland Security, Study on Mobile Device Security, at 27 (Apr. 2017).

[17] John Love, *A Brief History of Malware—Its Evolution and Impact*, LASTLINE (Apr. 5, 2018), https://perma.cc/ZCU8-FESK.

private sector and even the average American."[18] And the former NSA Director has called cyber espionage perpetrated through malware the "greatest transfer of wealth in history."[19] Allowing for devices with greater security protects against the variety of malware that threatens national security.

Malware can be simplified into three component parts: propagation, exploit, and payload. The payload, or the "desired malicious end such as to delete data or manipulate an industrial control system," may be different in each operation, but the initial stages of propagation and exploit look broadly similar across operations.[20] First, malicious code is delivered to a target system (propagation), here, via a mobile app. Second, it *exploits*, or alters, software programs already on the device, to take advantage of vulnerabilities in an operating system and allow the payload to execute. *Id.* at 305-07. *Third* comes the payload, which—as elaborated below—is the operative program that can achieve any of a variety of desired malicious ends when executed.

The grave consequences of malware for national security are demonstrated by

---

[18] Lily Hay Newman, *Security News This Week*, WIRED (June 5, 2021), https://perma.cc/5AHH-X8ES.

[19] Josh Rogin, *NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'* FOREIGN POLICY (July 9, 2012), https://perma.cc/CLH9-2DJC.

[20] Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model*, 8 J. NAT'L SEC. L. & POL'Y 301, 303 (2016).

three types of exploitations—(a) traditional malware that steals data; (b) ransomware that freezes data; and (c) Man-in-the-Middle attacks that disrupt data transmission.

a. Traditional Malware: These payloads allow bad actors to take "full remote control of an infected device."[21] They may steal financial information on a massive scale, through an individual app or an infected third-party app store.[22] Or they may access government systems[23] and protected information, such as code for malware developed by the NSA that could then be misused to perpetrate criminal activity.[24] Payloads may also gain access to sensitive or secure information on civilian and non-civilian government employees' devices[25] (a threat based on the content of the information itself and with the potential for blackmail), infiltrate apps designed for

[21] Olivia Beavers, *Researchers Identify Android Malware That Can 'Spy Extensively,'* THE HILL (Jan. 16, 2018), https://perma.cc/9KWM-XARD.

[22] Davey Winder, *Hacker Claims Popular Android App Store Breached: Publishes 20 Million User Credentials*, FORBES (Apr. 19, 2020), https://bit.ly/37FLZnN.

[23] *See* Andy Greenberg, *Chinese Spies Hacked a Livestock App to Breach US State Networks*, WIRED (Mar. 8, 2022), https://perma.cc/HC55-FAXR (describing Chinese hack of livestock app to access state government networks).

[24] Scott Shane et al., *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. TIMES (Nov. 12, 2017), https://perma.cc/472S-JC74.

[25] Ben Schreckinger, *How Russia Targets the U.S. Military*, POLITICOMAGAZINE (June 12, 2017), https://perma.cc/ZUV9-VHN7 (hacking NATO commander); Katie Benner et al., *Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa*, N.Y. TIMES (Dec. 3, 2021), https://perma.cc/6BL6-X8A4 (targeting U.S. embassy employees).

the military to track U.S. military movements[26] or the existence of military facilities,[27] and surveil the movement of U.S. government officials.[28] Finally, payloads may include intrusions on industrial control systems for critical physical infrastructure, such as major sources of water, electricity, or industrial plants.[29]

b. Ransomware: In a ransomware attack, an adversary freezes access to the device user's files in exchange for a ransom. If the user does not pay the ransom, the adversary may permanently delete the user's data. Per the White House, "[r]ansomware payments reached over $400 million globally in 2020, and topped $81 million in the first quarter of 2021."[30] For employees who use their personal mobile devices in the workplace (including government officials), ransomware poses a threat beyond the data contained on a device, as the ransomware may be transferred from a mobile device to a networked system via a shared wireless

---

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

[27] Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, THE GUARDIAN (Jan. 28, 2018), https://perma.cc/RN4R-6GG2.

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

[29] *E.g.*, Andy Greenberg, *Unprecedented Malware Targets Industrial Safety Systems in the Middle East*, WIRED (Dec. 14, 2017), https://perma.cc/Z6ZU-8HHF; Frank Bajak, *In Florida City, a Hacker Tried to Poison the Drinking Water*, AP NEWS (Feb. 8, 2021), https://bit.ly/3thIuMu.

[30] Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware, THE WHITE HOUSE (Oct. 13, 2021).

connection.[31] Ransomware attacks have hit a major oil pipeline in the United States and a major United States meat supplier, affecting domestic supply chains.[32] They have also "targeted entities that provide critical services" such as "hospitals and health care providers."[33] According to the Department of Homeland Security (DHS), "[r]ansomware attacks are on the rise and are becoming increasingly more sophisticated."[34]

c. Man-in-the-Middle Intrusions: In a Man-in-the-Middle attack, an adversary can "eavesdrop on the connection" "between an application and a remote server" and gain "the opportunity to alter data as it traverses the path, resulting in delivery of compromised information." *Id.* at 28. Such an intrusion occurred on iOS devices in 2015 via a third-party library. *Id.* at 29. Governments have also used Man-in-the-Middle attacks to "intercept and read bulk Internet traffic."[35]

* * *

[31] HIPAA Journal, Ransomware on Mobile Devices, https://perma.cc/6G27-J6NJ (last visited Mar. 31, 2022).

[32] Bree Fowler, *Ransomware Rises As a National Security Threat As Bigger Targets Fall*, C-NET (Oct. 18, 2021), https://perma.cc/X3ET-H5UQ.

[33] Testimony of National Cyber Director J. Chris Inglis, U.S. House of Representatives Comm. on Oversight & Reform, at 3 (Nov. 16, 2021).

[34] U.S. Dep't of Homeland Security, Study on Mobile Device Security, at 35 (Apr. 2017).

[35] *See Machine-in-the-Middle Attacks: What Are They, and How Can We Prevent Them?*, Internet Society (Mar. 24, 2020), https://perma.cc/3DVM-BPUK.

Apps are a key entryway for the cyber-based theft, disruption, and destruction described above, all of which threatens the United States' security. The national security implications of these attacks are twofold. First, malware affecting individuals' data on enough devices for a large-scale attack has national consequences. Second, as described above, malware in one mobile device may be transmitted to another mobile device, other types of devices (computers, infrastructure, etc.), or enterprise-scale networks. Attacks on larger-sized networks, whether on government servers or companies that are integral to defense, are national security issues. Heightened device security, such as that built into the App Store, protects against these two dangerous types of scenarios.

C. In Recognition Of The Growth Of Device-Based Threats, Cybersecurity Policy Has Become A Key National Priority.

It is worth noting that, based in part on the growth of device-based threats and foreign adversaries' use of cyber intrusions, cybersecurity is now a "top priority" and an "imperative across the government."[36] The list of security-centered agencies that have heavily invested in cybersecurity and committed to focus on cyber threats is long and growing.[37] The government's commitment to cybersecurity has also

---

[36] The White House, Interim National Security Strategic Guidance, at 18 (Mar. 2021).

[37] *E.g.*, *Cyber Threats from China, Russia, and Iran*: *Hearing before the Subcomm. on Cybersecurity, Infrastructure Protection, and Sec. Techs. of the H. Comm. on Homeland Sec.*, 113th Cong. 6 (2013) (Director of National Intelligence naming cyber the "top threat to U.S. National security"); Ellen Nakashima, *Pentagon*

extended to unprecedented public-private partnerships to invest in cyber defenses.[38] As recently as ten days ago, President Biden warned the private sector that foreign adversaries' "potential use of cybersecurity" is of "national interest," and stated that companies have "a patriotic obligation [] to invest as much as you can" to "buil[d] up [the] technological capacity to deal with . . . cyberattacks."[39] For the public-private partnership to build a robust cybersecurity framework, every bit of additional security, including Apple's App Store's existing protections, helps.

II. IF EPIC WERE TO PREVAIL, CONSUMERS AND THE COUNTRY WOULD BE SUBJECT TO HARMFUL NATIONAL SECURITY IMPLICATIONS AND ULTIMATELY WOULD BE WORSE OFF

A. Requiring Third-Party Apps Limits Consumers' Ability To Choose Heightened Device And National Security.

Epic's counterfactual world of requiring iOS mobile devices to permit

---

to Boost Cybersecurity Force, WASH. POST (Jan. 27, 2013), https://perma.cc/JNS2-L2TE (Department of Defense approving major expansion of its Cyber Command); About CISA, CISA, https://perma.cc/C9YZ-DLGR (last visited Mar. 31, 2022) (establishment of the Cybersecurity and Infrastructure Security Agency in 2018 to "coordinate[] the execution of our national cyber defense"); Response to Additional Prehearing Questions for Williams J. Burns Upon his Nomination to be Director of the Central Intelligence Agency, Senate Select Comm. on Intelligence at 7 (Feb. 19, 2021) (CIA Director committing to "making sustained investments" in cybersecurity).

[38] *See* D. Howard Kass, *Tech Heavyweights Vow Big Cybersecurity Investments, Enhancements*, MSSPALERT (Sept. 1, 2021), https://perma.cc/KU8E-JRL3 (describing how technology companies agreed to invest billions of dollars after meeting with President Biden to "raise the bar on cybersecurity").

[39] Remarks by President Biden Before Business Roundtable's CEO Quarterly Meeting, THE WHITE HOUSE (Mar. 21, 2022).

sideloading, or the downloading of applications through third-party app stores or directly onto a device, would make everyone worse off. It would deprive consumers of the ability to choose the highest-level device security. That restriction of choice would greatly increase the risks of cyber threats for individuals and, through scale- and network-based attacks, for the Nation. To the extent Apple could continue to have some level of app review, the practicalities of how court-enforced regulation would work present additional concerns.

While consumers cannot "choose" national security, they can take it into account when considering their own individual device security, as Appellant's own expert, *amici*, and its *amici*'s underlying sources have recognized.[40] Device security is a proxy for certain features of national security, like protection of an individual's data and networks (including data related to that individual's employer or contacts), privacy protections, and protections against eavesdropping, location tracking, or interference. Because device security and privacy features differentiate mobile devices and allow users greater freedom of choice, they are cognizable procompetitive antitrust concerns.

[40] *See* Trial Tr. 1689 (Evans) (Epic's expert conceding that "[p]rotecting iPhone users from security threats is a procompetitive benefit"); *see also* EFF Br. 14; Law, Economics, and Business Professors' Br. 11 (citing Erika M. Douglas, *Data Privacy Protection as a Procompetitive Justification*, 36 Antitrust 1, 12 (Dec. 2021) (explaining that when a "justification is tied to improving the quality of privacy through competition . . . it is likely to be cognizable in antitrust law")).

Limiting consumers' choices to only devices with lower mobile app security decreases competition and increases risks to national security. Apple is not "forc[ing] consumers" to "buy security and privacy benefits that they might not want." Law, Economics, and Business Professors' Br. 7. Security is a factor that consumers can and do consider when choosing a mobile device. Apple chose to place a high priority on security in its app distribution ecosystem.[41] Other platforms may make different decisions. Good Old Games likely assigns security a lower priority because its purpose is "to make unworkable games work again."[42] Android may emphasize app diversity over security or user privacy if it prioritizes ad revenue, because ads rely on "the ability of an app to track user behavior." *Id.* Consumers should be allowed to choose a more secure device platform that limits risk of national threats from foreign adversaries' scale- and network-based attacks described in Section I.

Even if, in Epic's counterfactual world, the App Store may continue to perform some level of vetting, such a nebulous result would turn antitrust law into

[41] *See, e .g.*, Trial Tr. 3360 (Federighi) (stating that from the beginning Apple designed the iOS system as an "end-to-end system that could give customers . . . confidence" in security when downloading apps, knowing that users would download software at a greater rate than macOS (laptop) users); Dkt 742-5 ¶¶ 29, 32 (Rubin) (explaining Apple's "App Review and app distribution" layers of security, wherein apps are reviewed by computer and manual human review, in addition to "on-device security").

[42] Dkt. 742-5 ¶ 84 (Rubin).

an unwanted and risky regulatory mechanism. "No court should impose a duty to deal that it cannot explain or adequately and reasonably supervise."[43] Epic's own expert testified that, if Epic prevailed, the court would need to "consult with security experts and people who are experts in content moderation" to determine an acceptable level of security for the App Store.[44] In other words, courts would be required to supervise security measures with national security consequences on a continued basis, and constantly evaluate tradeoffs between security and ease of access to third-party apps. It is not the judiciary's role to fashion a remedy that raises national security questions every time new technological advancements or security threats arise.

The regulatory nature of Epic's desired outcome is all too apparent, as forced sideloading is currently at issue in pending legislation. *See, e.g.*, S. 2992, the American Innovation and Choice Online Act, and S. 2710, the Open App Markets Act. The national security implications of forced sideloading are front and center in debates on these bills. Members of Congress have criticized their "potential national security consequences,"[45] and former intelligence officials have warned that the

[43] Phillip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 853 (1989).

[44] Trial Tr. 2709-12 (Mickens).

[45] U.S. Antitrust Legislative Proposals: A Global Perspective, U.S. CHAMBER OF COMMERCE (Feb. 16, 2022), https://perma.cc/R3UD-4ZEU.

legislation would "potentially put sensitive U.S. data and IP in the hands of Beijing."[46] Trade and industry groups have seconded these concerns.[47] Rather than leave this kind of regulation to Congress, where it belongs, Appellant invites the Court to jump into the legislative fray. The Court should decline that invitation.

To summarize, courts should not impede national security objectives where the legal basis for doing so does not exist. The antitrust laws are "concerned with the protection of competition, not competitors." *Brown Shoe Co. v. United States*, 370 U.S. 294, 320 (1962). If Epic were to prevail, competition for higher quality device security would be stifled, and courts would be forced into unwanted regulatory postures that would open the door for greater risk of security threats. This Court should not condone either outcome.

B. Requiring A Lower Standard Of Security Would Place Individuals And The Country At Risk.

The world in which Epic prevails also immediately places individuals and the country at risk. *First*, Epic's proposed outcome runs directly counter to the "best practices" identified by the executive and legislative branches for mitigating mobile

---

[46] Letter from Robert Cardillo, Former Director, National Geospatial-Intelligence Agency, et al., to Nancy P. Pelosi, Speaker of the House, and Kevin O. McCarthy, House Minority Leader, at 1 (Sept. 15, 2021).

[47] *E.g.*, White Paper on National Security Issues Posed by House Antitrust Bills, Computer & Commc'ns Indus. Ass'n (Sept. 2021) ("[T]hese bills . . . may inadvertently undermine U.S. national security" and "weaken the U.S.'s ability to counter foreign cyber attacks, espionage, influence and surveillance efforts.").

security threats.[48] DHS has explicitly stated that "users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorized app stores,"[49] and has praised "security architecture improvements across all the mainstream mobile . . . operating systems . . . because they increase resilience to attack and raise the level of difficulty and the cost for attackers." *Id.* at 22. In 2020, the Committee on Oversight and Reform of the U.S. House of Representatives told Apple and other developers that they "can and must do more to ensure that smartphone applications made available to U.S. citizens on the AppStore protect stored data from unlawful foreign exploitation, and do not compromise U.S. national security."[50] And in 2021, President Biden signed an executive order on "[i]mproving the Nation's cybersecurity" that directed the federal government to adopt and implement a new type of cyber security model that is utterly inconsistent with Epic's proposed outcome.[51] Epic's proposal looks backwards, not forwards, and would

[48] U.S. Dep't of Homeland Security, Study on Mobile Device Security, at 37 (Apr. 2017).

[49] *Id.*; *see id.* at 32 ("[A]pp security review still requires skilled analysts and manual investigation.").

[50] Letter from Stephen F. Lynch, Chairman, Subcomm. on Nat'l Sec., U.S. House of Representatives Comm. on Oversight & Reform, to Timothy Cook, CEO, Apple Inc., at 3 (July 14, 2020).

[51] Executive Order on Improving the Nation's Cybersecurity, THE WHITE HOUSE § 3 (May 12, 2021) (requiring agencies to "develop a plan to implement Zero Trust Architecture"). Zero Trust Architecture is a security model that continually "looks

redound to the detriment of all by prohibiting the very device security touted by the President, DHS, and Congress.

Second, requiring Apple devices to accept third-party apps and app stores necessarily increases the risk of malware on iOS devices, which directly correlates to an increased risk to national security. For example, "iOS is the only computing platform today where ransomware effectively doesn't exist," because Apple does not allow third-party apps to access the entire storage volume of a user device.[52] But "the most common infection vector is downloading ransomware-infected apps from third party app stores." *Id.* (internal quotation marks and citation omitted). Similarly, Apple's expert opined on a reputable trade security report that has found incidences of observed malware in Apple iOS devices are fewer than those in Android devices.[53] As the former director of the CIA and NSA has stated, opening the App Store will "inadvertently undermine such protections and increase risks to

---

for anomalous or malicious activity" and restricts access until programs are proven trustworthy because the model "assumes that a breach is inevitable." *Id.* § 10(k).

[52] Letter from Timothy Powderly, Senior Director of Gov't Affairs, Americas, Apple Inc., to Senator Dick Durbin, Chairman, Comm. on the Judiciary, et al. (Mar. 3, 2022).

[53] Trial Tr. 3750-53 (Rubin) (describing 2020 Nokia Threat Intelligence Report and explaining that the difference in malware rates is attributed to "the availability of multiple app stores in Android"); DX4975 (Nokia Report) at 8 (showing observed malware infections in the industry occurring on 1.7% of iOS devices compared to 26.6% of Android devices).

average users."[54] At scale or when transferred to enterprise-level networks, those risks become national security concerns.

Relatedly, the security risks to everyone, including non-iOS users, will increase. Because cybersecurity is mostly a private good impacting the public, its negative externalities are of national concern.[55] An adversarial operation on *any* single user's device is a tear in the Nation's security fabric writ large. Further, as explained above, a malware infection on one device can "infect other phones and other users."[56] So even if only a few iOS users download third-party apps and the rest continued to use iOS devices without sideloading, iOS users who do not sideload could become vectors of cyber intrusions. For that reason, the "size and scope" of potential intrusions from foreign adversaries could "dwarf[]" that of "past app-based espionage campaigns."[57] The risks are difficult to comprehend, as some vulnerabilities, such as botnets, can lie dormant for years before they are activated

---

[54] Michael Hayden, *Changing How App Stores Operate Could Have National Security Implications*, THE CHERTOFF GROUP (Aug. 5, 2021), https://perma.cc/YL68-2GHY.

[55] *See* Paul Rosenzweig, Cybersecurity and Public Goods, The Public/Private "Partnership," in *Emerging Threats in National Security and Law*, at 2 (Hoover Institution 2011) ("core national security functions . . . are all dependent, to greater or lesser degrees, on the resilience of the private-sector networks").

[56] Trial Tr. 3736 (Rubin).

[57] Michael Hayden, *Changing How App Stores Operate Could Have National Security Implications*, THE CHERTOFF GROUP (Aug. 5, 2021), https://perma.cc/YL68-2GHY.

and do harm.[58] In sum, it is incorrect to think that iOS users who do not sideload or non-iOS users will be unaffected by the national security consequences of Epic's desired outcome.

Third, contrary to the supposition of Appellant's *amici* (*see* EFF Br. 2, 12), permitting third-party app stores actually decreases, rather than increases, innovation in security. Technology companies are at the forefront of cybersecurity, often in a position to learn of vulnerabilities and trends before the government is. Allowing each company to determine its own level of investment in security features encourages those who want to make security a priority, like Apple, to allocate resources to that aspect of their products. This benefits consumers, the Nation, and the industry. As the saying goes, a rising tide lifts all boats. For example, Apple mandated "Privacy Nutrition Labels," which required apps to disclose their data collection practices, and five months later, Google mandated its own version of privacy labels.[59] Reflecting, perhaps, a robust competition for security, Google also

[58] *What Is a Botnet?*, PANDA SECURITY (Dec. 5, 2017), https://perma.cc/6EU6-XPWU.

[59] *Compare* Melanie Weir, *What are Apple's Privacy Nutrition Labels?*, TECH (Jan. 20, 2021), https://perma.cc/V47Q-C73V, *with* Sergiu Gatlan, *Google Play Store to Add Privacy Information for All Android Apps*, BLEEPINGCOMPUTER (May 6, 2021), https://bit.ly/3u3pWyR.

cracked down on apps that did not meet a minimum level of safety, reducing the number of blacklisted apps in the Play store in 2020 by 60%.[60]

If Epic's antitrust theory prevailed in this Court, those nutrition labels could not be mandated on all apps offered to iOS users, and Google might not feel compelled to tighten its own app screening process. The industry-wide standards for security would be set back years, if not decades. This is the kind of outcome that would "chill desirable activity," reduce "incentives for innovation," and contradict the "general policy limitations" inherent in antitrust law.[61]

Appellant's *amici* claim that Apple prioritizes security for threats from social engineering over other types of security. *See* EFF Br. 15-16.[62] Whether or not that's true, that point favors the world in which Apple maintains its App Store restrictions, not Epic's desired world. All manner of malware propagation are legitimate targets of concern that could result in payloads of national security concern. Other developers are free to optimize for threats from other sources and foster competition

---

[60] 2020 Mobile App Threat Landscape Report, RiskIQ, at 5 (2021); *see* U.S. Dep't of Homeland Security, Study on Mobile Device Security, at 36 (Apr. 2017) (stating both Google and Apple have "made continuous improvements in their security processes, including app vetting, a cornerstone of their business models").

[61] Phillip Areeda, *Essential Facilities: An Epithet in Need of Limiting Principles*, 58 ANTITRUST L.J. 841, 851 (1989).

[62] *See also, e.g.*, Brian Barrett, *How 18 Malware Apps Snuck Into Apple's App Store*, WIRED (Oct. 25, 2019), https://perma.cc/D6JS-QDHV (private security group founder surmising that Apple does not prioritize combating adware).

in the marketplace while increasing the overall level of security afforded to device users.[63] That is competition par excellence.

Fourth, requiring all app stores to conform to the same type of security by mandating allowance of third-party applications increases national security risk by creating a monoculture security environment. In Epic's world, nearly every mobile device in the United States would be subject to identical security risks from forced sideloading, and over 50% of all mobile devices used in the United States (those using Apple's iOS system) would be forced to have identical (and potentially weaker) security features.[64] If more than 50% of devices operate the same security measures, their uniform vulnerabilities expose the nation to cyber intrusions on an enormous scale. Imagine the significant economic consequences if 100 million people suddenly could not access their credit card accounts at the same time, or if that many devices were conscripted into a malicious botnet. That is why "single

[63] Apple's security is not perfect. *See, e.g.*, Reed Albergotti & Chris Alcantara, *Apple's Tightly Controlled App Store Is Teeming with Scams*, WASH. POST (June 6, 2021), https://perma.cc/M2HG-33PU. Nor are its security choices above critique. *See* Paul Rosenzweig, *Kenny Rogers, China, and the Tech Business*, THE HILL (Jan. 19, 2022), https://perma.cc/RD7D-66JQ. The fact that there is no single right way to prioritize national security on mobile devices is all the more reason why antitrust law should not stymie companies' choices to explore new and differing ways of promoting security features.

[64] *Mobile Operating System Market Share United States of America*, Feb. 2021 – Feb. 2022, STATCOUNTER, https://perma.cc/PQ9H-BDE5 (last visited Mar. 31, 2022).

collaboration and communications system[s]" are disfavored in the world of cybersecurity, because "the costs of a single-point-of-failure monoculture" may be greater than efficiency benefits.[65]

CONCLUSION

The judgment of the district court on the Sherman Act claims should be affirmed.

Dated: March 31, 2022

Respectfully submitted,

/s/ Roy T. Englert, Jr.

Roy T. Englert, Jr.
Leslie C. Esbrook
ROBBINS, RUSSELL, ENGLERT, ORSECK, & UNTEREINER LLP
2000 K Street NW, 4th Floor
Washington, D.C. 20006
Tel.: (202) 775-4500
renglert@robbinsrussell.com
Counsel for Amici Curiae

[65] Paul Rosenzweig, *The Cyber Monoculture Risk*, LAWFARE (Oct. 1, 2021), https://perma.cc/9QSX-TZDX.

APPENDIX: List of *Amici Curiae*

1. Paul Rosenzweig served as Deputy Assistant Secretary for Policy in the Department of Homeland Security.

2. General (ret.) Michael V. Hayden, United States Air Force, served as the Director of the Central Intelligence Agency and as Director of the National Security Agency.

3. John O. Brennan served as Director of the Central Intelligence Agency. He previously served as Deputy National Security Advisor for Homeland Security and Counterterrorism and Assistant to the President.

4. Richard A. Clarke held senior national security positions in the U.S. government for nearly 30 years, including over a decade in the White House, where he served as Special Advisor to the President for Cyberspace; National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism; and Special Assistant to the President for Global Affairs.

5. Rudy de Leon served as Deputy Secretary of Defense at the Department of Defense.

6. Steven Weber is a Professor of the Graduate School and former Director of the Center for Long Term Cybersecurity at the University of California Berkeley. He is also a Partner at Breakwater Strategy in Washington DC.

7. Richard H. Ledgett Jr. served as Deputy Director of the National Security Agency.

8. Harvey Rishikof is a Visiting Professor of Law at Temple University Beasley School of Law. He previously served as Senior Policy Advisor at the Office of the Director of National Intelligence, Director of Military Commissions and Convening Authority at the Department of Defense, and Legal Counsel to the Deputy Director of the FBI.

9. Roger Cressey served as Chief of Staff for the President's Critical Infrastructure Protection Board and as Director for Transnational Threats on the National Security Council.

10. William Evanina is founder and CEO of the Evanina Group, LLC and served for six years as the Director of the National Counterintelligence and Security Center within the Office of the Director of National Intelligence.

11. Frank Cilluffo is the Director of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. He formerly served as Special Assistant to the President for Homeland Security and as Commissioner of the U.S. Cyberspace Solarium Commission.

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

13. Gary Corn is the Director of the Technology, Law & Security Program at American University Washington College of Law. He previously served as Staff Judge Advocate (General Counsel) at U.S. Cyber Command.

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

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

16. Timothy H. Edgar is a Senior Fellow at Brown University's Watson Institute for International Studies and Public Affairs and serves as Director of Graduate Studies for Brown University's M.Sc. in Cybersecurity. He has also served as Director of the Cybersecurity Directorate of the National Security Staff at The White House.

17. Richard Mogull is Analyst & CEO of Securosis, a leading independent security research and advisory firm.

18. Tatyana Bolton served as a Senior Official at the U.S. Cybersecurity and Infrastructure Security Agency.

19. Diane Rinaldo served as the Cybersecurity and Technology Advisor to the U.S. House of Representatives' Permanent Select Committee on Intelligence. She previously served as Administrator and Assistant Secretary (Acting) for the National Telecommunications and Information Administration of the U.S. Department of Commerce.

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

21. Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University. He is also the former Chief Technologist at the Federal Trade Commission.

22. Ambassador James Jeffrey is the former Deputy National Security Advisor.

23. Vice Admiral (ret.) J. Michael McConnell, United States Navy, served as the Director of National Intelligence and Director of the National Security Agency.

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) 21-16506, 21-16695

I am the attorney or self-represented party.

This brief contains 5,943 **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/Roy T. Englert, Jr. **Date** Mar 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 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 March 31, 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: March 31, 2022

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