No. 21-12835

United States Court of Appeals for the Eleventh Circuit

APPLE INC.,

Plaintiff-Appellant,

v.

CORELLIUM, INC.,

Defendant-Appellee.

On Appeal from the United States District Court for the Southern District of Florida, No. 9:19-cv-81160-RS (Hon. Rodney Smith)

CORRECTED BRIEF OF DEFENDANT-APPELLEE [REDACTED VERSION]

Seth D. Greenstein
CONSTANTINE CANNON LLP
1001 Pennsylvania Ave, NW
Suite 1300N
Washington, DC 20004
(202) 204-3514

Justin B. Levine
COLE, SCOTT & KISSANE, P.A.
Esperante Building
222 Lakeview Avenue, Suite 120
West Palm Beach, Florida 33401
(561) 612-3459

Thomas C. Goldstein
Kevin K. Russell
GOLDSTEIN & RUSSELL, P.C.
7475 Wisconsin Avenue
Suite 850
Bethesda, MD 20814
(202) 362-0636

Counsel for Defendant-Appellee Corellium, Inc.

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Rule 26.1-1, Defendant-Appellee certifies that it has no parent corporation and no publicly held corporation holds 10 percent or more of its stock.

Pursuant to Eleventh Circuit Rule 26.1-2(a) and (b), Defendant-Appellee certifies that Plaintiff-Appellant's Certificate of Interested Persons is correct and complete, apart from Defendant-Appellee's corporate name change, which the Court recognized in its Jan. 31, 2022 Order substituting the party name and amending the caption:

Corellium, Inc.: Appellee

February 10, 2022

/s/ Kevin K. Russell
Kevin K. Russell

Counsel for Defendant-Appellee

STATEMENT REGARDING ORAL ARGUMENT

Pursuant to Rule 34(a)(1) of the Federal Rules of Appellate Procedure and Rules 28-1(c) and 34-3(c) of the Eleventh Circuit Rules, Defendant-Appellee Corellium, Inc. requests oral argument. The case raises important questions regarding the application of the fair use doctrine to computer software. The Court's decision-making would benefit from holding oral argument.

TABLE OF CONTENTS

TABLE OF AUTHORITIES[*]

Cases

[*] Authorities upon which Defendant-Appellee primarily relies are marked with an asterisk.

Constitutional Provisions

Statutes

Regulations

Other Authorities

STATEMENT OF THE ISSUES

1. Whether the district court erred in granting Defendant-Appellee Corellium, Inc.'s motion for summary judgment against Apple's claim for direct copyright infringement under the fair use doctrine codified at 17 U.S.C. § 107.

2. Whether Apple preserved any separate argument regarding the fair use doctrine's application to its contributory infringement claims.

3. If so, whether the district court erred in granting summary judgment on fair use grounds against Apple's claims of contributory infringement.

INTRODUCTION

Defendant-Appellee, Corellium, Inc., developed and markets a software product called the "Corellium Security" product (CORSEC). The program enables researchers to study in detail the operating system software embedded in mobile devices. This case involves CORSEC's use for analyzing Apple's iOS, the operating system that runs the iPhone. CORSEC itself contains no copyrighted Apple code. Instead, the program allows researchers to run iOS files—which Apple makes available for free download on the internet, without licensing restrictions—on specialized servers Corellium sells to customers or on cloud-based servers maintained by Corellium.

CORSEC is used by researchers, federal agencies, defense contractors, and private companies like [redacted].[1] Although customers can use the tool, and the knowledge gained from it, for a variety of purposes, its principal use is for cybersecurity research. CORSEC is an invaluable tool for such research not simply because it allows users to

[1] All material filed under seal references or contains information that was sealed in the district court.

run iOS on a different hardware platform, but because it includes a set of tools and capabilities absent in iOS itself, such as the ability to view system calls in real time, pause operations, and modify the system kernel. These and other capabilities allow researchers to gain a deep understanding of how iOS works and what its vulnerabilities may be.

Copying, using, and modifying software in order to reverse engineer or otherwise understand the software's functional elements has long been considered fair use. *See, e.g.*, *Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183, 1198-99 (2021) (collecting citations); U.S. Copyright Office, *Software-Enabled Consumer Products: A Report of the Register of Copyrights* 42 (Dec. 2016) (endorsing copying computer code for security research as fair use).

Corellium does not compete with Apple for iOS users. For ordinary consumers, CORSEC is inferior to an iPhone running standard iOS in every material respect, lacking the mobility and core functionalities of an ordinary mobile device (like the ability to send a text, make a phone call or run graphic-intensive games), while costing far more. CORSEC exists because it serves a completely different purpose and provides a distinct set of capabilities that are useful only to researchers trying to understand the details of how iOS functions.

Apple points to the possibility that knowledge of how its operating system works (or fails to work) can help third parties create "exploits" to compromise the security of Apple devices. But as the district court noted, Corellium takes steps to minimize the chance that the knowledge gained from its products will be misused. And Apple has provided no evidence that any vulnerability discovered using CORSEC has ever been used for illicit purposes, much less that Corellium has encouraged such use. At the same time, Apple fails to acknowledge that such "exploits" are routinely used for legitimate purposes, including security research and law enforcement.

In the end, Apple is asserting that its copyright in iOS gives it the right to control the terms under which independent parties can effectively research the security of its software—for example, requiring that exploits be reported to Apple rather than used for law enforcement purposes. Preventing such overreach is the office of the fair use doctrine. The district court rightly applied the doctrine in this case to prevent

Apple's copyright from unjustifiably interfering with copyright law's core goal of fostering the discovery and dissemination of knowledge.

STATEMENT OF THE CASE

I. Factual Background

A. Apple's Devices And Copyrighted Software

Apple uses iOS as the operating system for its iPhone, iPod Touch, and early iPad devices. Doc. 783, pg. 3. The heart or "kernel" of iOS is open-source software that was not developed solely by Apple. *Id.*, pg. 4. Apple asserts copyright protection in multiple versions of iOS for the code it added, and for certain of its wallpaper images and icons. Br. 5-6.

In some respects, Apple goes to great lengths to control how its customers use their devices. For example, iOS prevents users from installing software on their iPhones through any means other than Apple's proprietary App Store, where it generally charges a 30% commission. Doc. 783, pg. 7; *Epic Games, Inc. v. Apple Inc.*, --- F. Supp. 3d ----, 2021 WL 4128925, at *21, *81 (N.D. Cal. Sept. 10, 2021) (finding commission rate "supracompetitive"), *appeal pending*, No. 21-16506 (9th Cir. docketed Sept. 13, 2021). Apple also includes extensive measures to prevent anyone from altering that or any other aspect of iOS without Apple's permission. Doc. 783, pgs. 6-7.

In other respects, Apple takes a decidedly hands-off approach to how its products are used. Apple offers its users powerful tools for keeping their communications and other data secret, *see, e.g.*, Doc. 472-4, pg. 122; Doc. 472-31, pgs. 93-94, features especially useful to criminals and other bad actors. Although Apple's products can be used maliciously in the wrong hands, Apple engages in no vetting or monitoring of its customers, selling to almost anyone able to pay for its devices and priding itself on respecting customers' privacy once the devices are sold. *See* Doc. 783, pg. 32; Government's Motion to Compel Apple Inc. to Comply with This Court's February 16, 2016 Order Compelling Assistance in Search, *In re the Search of an Apple iPhone*, No. 5:16-cm-00010 (C.D. Cal. Feb. 19, 2016) (seeking court order to overcome Apple's refusal to cooperate in unlocking iPhones of suspected terrorists).

B. Security Research On iOS

Despite its efforts, Apple cannot find or fix all of the flaws in iOS's security features by itself. Identifying those flaws and assessing their impacts is the goal of security researchers, including researchers who work for the government, academic institutions, and private companies that use Apple software. Doc. 783, pg. 8.

Security researchers seek to identify software flaws that can be used for so-called "exploits" that evade Apple's security measures and allow access to aspects of a device or its data. Exploits may be used for nefarious or socially beneficial purposes. For example, exploits are used by cybercriminals to steal data or install viruses or ransomware. For that reason, and in acknowledgment that it needs assistance policing its software, Apple invites researchers to submit exploits they develop to its Security Bug Bounty Program, and pays handsomely for the most serious flaws researchers find. Doc. 783, pg. 8; Doc. 472-31, pgs. 79-84; Doc. 1, pg. 2 (Apple bounty program offers up to $1 million per exploit).

Exploits can also be used lawfully for socially beneficial purposes. In 2010, over Apple's objection, the Copyright Office determined that "jailbreaking" devices to circumvent limitations that prevent consumers from installing lawfully obtained third-party applications is legal under the Digital Millennium Copyright Act (DMCA) and a fair use under the Copyright Act. *See* 75 Fed. Reg. 43,825, 43,828-30 (July 27, 2010); 37 C.F.R. § 201.40(b)(9).

Security researchers similarly use exploits to jailbreak iPhones in order to install the software they need to conduct further security research. *See* Doc. 817-5, pgs. 206-08. Creating exploits also is an essential part of security research, as only bugs that can be exploited implicate security concerns. That is why the National Institute of Standards and Technology, a federal agency, requests exploit examples be submitted as part of its Mobile Threat Catalogue.[2] It is also why Apple requires that every submission to its bounty program include an exploit demonstrating that the identified flaw is sufficiently serious to merit a bounty payment.[3]

Law enforcement and national security agencies also buy exploits to bypass Apple's security measures and recover evidence of serious crimes or threats. Doc. 472-31, pg. 84; Doc. 472-6, pgs. 254-55; *see also* Kristin Finklea, Cong. Rsch. Serv., R44827, *Law Enforcement Using and*

[2] *See* Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, Mobile Threat Catalog: Contributing, https://pages.nist.gov/mobile-threat-catalogue/contributing.html (last visited Feb. 9, 2022).

[3] *See* Apple Developer, Apple Security Bounty, https://developer.apple.com/security-bounty/ (last visited Feb. 9, 2022).

Disclosing Technology Vulnerabilities 6, 13 (2017)[4]; Brian Fung, *The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities*, Wash. Post (Aug. 31, 2013).[5]

C. Corellium's Research Tool

Defendant Corellium's CORSEC software is a research tool for analyzing mobile device operating systems and applications. Doc. 783, pgs. 1, 8. A principal use for the tool is cybersecurity research. *Id.*, pgs. 1, 24. In fact, Forbes named CORSEC the best cybersecurity product of the year in 2020.[6] Researchers using the tool have been responsible for alerting Apple and the public to numerous serious iOS vulnerabilities. *See* Doc. 472-1, pg. 188; Doc. 472-13, pgs. 206, 278-79.

[4] https://sgp.fas.org/crs/misc/R44827.pdf.

[5] https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

[6] *See* Thomas Brewster, *Forbes Cybersecurity Awards 2020: Corellium, the Tiny Startup Driving Apple Crazy*, Forbes (Dec. 27, 2020), https://www.forbes.com/sites/thomasbrewster/2020/12/27/forbes-cybersecurity-awards-2020-corellium-the-tiny-startup-driving-apple-crazy/?sh=6651113329e4.

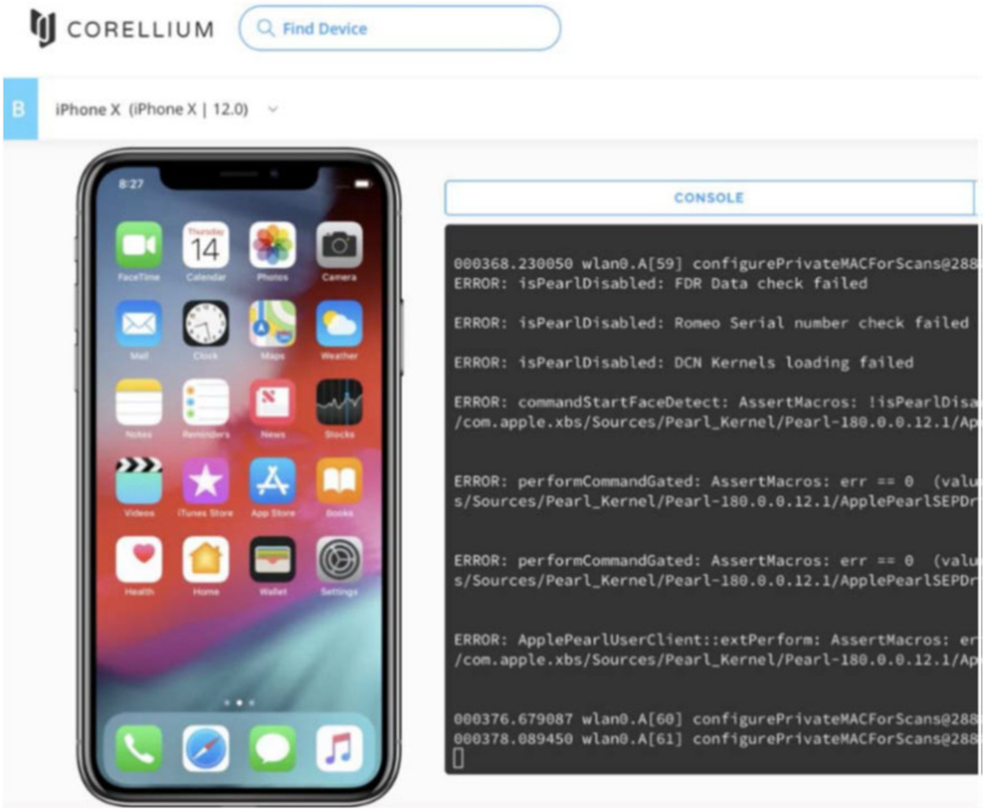
CORSEC itself contains no copyrighted Apple code. Doc. 472-14, pg. 66; Doc. 472-1, pg. 71. Nor does Corellium sell iOS to its users. Instead, customers obtain the particular versions of iOS they wish to analyze directly from Apple, which allows the public to download the complete code of any current or obsolete version of iOS as a unitary "IPSW" file—for free, and without a license, registration, or password—from a publicly available website, https://ipsw.me. Doc. 783, pgs. 5, 11-12.[7]

Once the users select the version of iOS they wish to test (*e.g.*, version 14.7.1), and a particular iPhone to run it on (*e.g.*, iPhone 11), CORSEC then creates "tailored, virtual models of iPhones using iOS files loaded by the user." Doc. 783, pg. 1.[8] Specifically, the system modifies the relevant iOS files to make them interoperable with CORSEC and creates a "virtual" environment in which users can analyze the iOS code,

[7] Corellium once provided a USB drive that included both the CORSEC software and some of the freely available IPSW files to [redacted]. Doc. 470-18, pgs. 184-85; Doc. 470-31; Doc. 472-13, pgs. 221-22.

[8] Corellium also produces versions that virtualize non-Apple Android and Linux devices. Doc. 783, pg. 1.

observe iOS in operation, and test their own iOS-based applications on computers rather than iPhones. Doc. 783, pgs. 11-13. To enable these investigations, CORSEC provides a suite of tools unavailable in iOS itself. For example, the CoreTrace feature provides a console with step-by-step descriptions of "system calls," otherwise invisible steps the operating system takes to execute commands and run applications:



```
000368.230050 wlan0.A[59] configurePrivateMACForScans@288
ERROR: isPearlDisabled: FDR Data check failed

ERROR: isPearlDisabled: Romeo Serial number check failed

ERROR: isPearlDisabled: DCN Kernels loading failed

ERROR: commandStartFaceDetect: AssertMacros: !isPearlDisa
/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/Ap


ERROR: performCommandGated: AssertMacros: err == 0  (valu
s/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDr


ERROR: performCommandGated: AssertMacros: err == 0  (valu
s/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/ApplePearlSEPDr


ERROR: ApplePearlUserClient::extPerform: AssertMacros: er
/com.apple.xbs/Sources/Pearl_Kernel/Pearl-180.0.0.12.1/Ap


000376.679087 wlan0.A[60] configurePrivateMACForScans@288
000378.089450 wlan0.A[61] configurePrivateMACForScans@288
```

Doc. 56, pg. 12. Using CORSEC, researchers can also "halt execution of the virtual device, amend the kernel, look at lists of files, clone snapshots, among other things—giving great introspection into aspects of iOS and its operation on iOS devices." Doc. 783, pg. 23; *see also id.*, pg. 21.

As should be obvious, CORSEC is no substitute for iOS running on an iPhone. The virtualized iPhones have "relatively limited functionality." Doc. 783, pg. 1. They cannot make phone calls, send text messages, use face or fingerprint identification features, download applications from the App Store, or run certain graphic-intensive applications. *Id.*, pgs. 1, 3; Doc. 472-3, pgs. 51-52.

D. Corellium's Licensees

CORSEC has been used by major corporations (*e.g.*, [redacted]) and defense contractors (*e.g.*, [redacted]), as well as by private security research firms and [redacted]. Doc. 472-29, pgs. 26-27; Doc. 472-32, pgs. 79-81, 136-38. Corellium sells to customers directly and through a well-known software security firm, Azimuth Security, [redacted]. Doc. 783, pg. 9; Doc. 472-14, pgs. 53-54, 107.

Corellium vets its customers and refuses to license CORSEC where it has reason to believe it might be used for unlawful or bad faith research activities. Doc. 783, pgs. 9-10; Doc. 472-13, pg. 208; Doc. 472-14, pg. 123. While Corellium markets CORSEC's ability to discover vulnerabilities that can then be sold (*e.g.*, to Apple's bounty program), it has never encouraged sales of exploits for illegal or harmful uses. Doc. 472-13, pg. 207. To the contrary, Corellium's licensing agreement prohibits using CORSEC for illegal purposes, a restriction it has previously enforced by terminating access to its product. *See* Doc. 783, pg. 10; Doc. 553-18, § 1.3; Doc. 472-13, pgs. 207-09.

E. Apple's Prior Relationship With Corellium And Its Founders

In 2018, Corellium demonstrated CORSEC to Apple. Doc. 783, pg. 13. After conducting due diligence, Apple offered to purchase the company, envisioning several internal uses for its software. *Id.*, pgs. 2, 13-14; Doc. 472-2, pg. 5. Corellium rejected Apple's offer. Doc. 470-4, pg. 6.

Approximately a year later, Apple sued Corellium, claiming that CORSEC infringes Apple's copyright in iOS. Doc. 783, pg. 14. Just before filing its complaint, Apple announced it would release to certain developers a security research device (a modified iPhone) with some research functions. Doc. 518-4, pgs. 11-12. An Apple executive admitted that [redacted]. Doc. 472-4, pgs. 90-91. In June 2021, nearly six months after the district court entered summary judgment against it, Apple announced development of its Xcode Cloud software which will allow Apple Developers to automate the process of commercial application development and distribution.[9] Apple does not market Xcode Cloud as a tool for security research.[10]

II. Procedural History

Apple twice amended its complaint, adding a claim under the Digital Millennium Copyright Act (DMCA). Docs. 56, 589. On May 12, 2020, Corellium filed a Motion for Summary Judgment against all of Apple's claims, and Apple filed a Motion for Partial Summary Judgment as to its DMCA claim. Docs. 464, 470. On December 29, 2020, the district court granted Corellium summary judgment against Apple's infringement claims, finding that CORSEC made fair use of Apple's copyrighted works. Doc. 783, pg. 33. The court denied summary

[9] *See* Press Release, Apple, Apple Introduces New Developer Tools and Technologies to Create Even Better Apps (June 7, 2021), https://www.apple.com/newsroom/2021/06/apple-introduces-new-developer-tools-and-technologies-to-create-even-better-apps/.

[10] *See* Apple Developer, Xcode Cloud, https://developer.apple.com/documentation/Xcode/Xcode-Cloud (last visited Feb. 9, 2022).

judgment to both parties on Apple's DMCA claims, finding disputed questions of material fact. *Id.*, pgs. 37-38.[11]

On August 17, 2021, the district court entered final judgment after the parties stipulated to dismissing Apple's DMCA claim and Corellium's counterclaims. Doc. 1013. In the stipulation, Apple waived its claims for money damages on its copyright claims, limiting this appeal to its request for prospective injunctive relief. *Ibid*.

[11] [redacted]

SUMMARY OF ARGUMENT

Corellium's research tool makes transformative use of Apple's copyrighted computer code in order to provide researchers deep insights into iOS's functionality. Because that transformative use does not materially diminish Apple's incentives to produce or improve its operating system, Corellium is entitled to invoke the Copyright Act's exemption for fair use.

I. Starting with the first statutory fair use factor, copying to "shed[] light on an earlier work" is an established transformative use. *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994); *see also* 17 U.S.C. § 107 (giving "research" and "scholarship" as examples of fair use). Applying that principle to the computer context, courts and the Copyright Office have long recognized that copying software to reverse engineer it or reveal its functionality is a transformative, fair use. That is exactly what CORSEC does—it allows researchers to observe the otherwise inaccessible details of iOS's functioning so they can understand how it works and what its vulnerabilities might be. Apple's contrary claim that Corellium simply offers iOS "in a different format," Br. 18, is belied by the record and common sense. No one would pay thousands of dollars to run software designed for a mobile phone on a computer that is vastly less portable and capable than the phone she already has in her pocket.

The second factor weighs in favor of fair use because computer code, while having some expressive qualities, falls outside the core of what copyright is intended to protect. In addition, overbroad copyright protection in an operating system creates a special risk that copyright owners will stifle competition in other markets (here, the markets for application sales and security research).

The third factor weighs in favor of fair use where the amount of computer code used is "tethered to a valid, and transformative, purpose." *Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183, 1205 (2021). Here, if CORSEC is to perform its transformative purposes as a research tool, users must be able to copy, run, observe, and modify substantial portions of the system software.

There is no evidence that this use materially affects the fourth factor, "the potential market for or value of the copyrighted work." 17 U.S.C. § 107(4). There is no market for iOS itself—Apple gives it away as a free download on the internet. And even if Apple could rely on CORSEC's effect on the market for iPhones—which it cannot, as iPhones are neither the "copyrighted work" nor a derivative of that work—there is zero evidence that CORSEC is driving down demand for iPhones in any way that materially affects Apple's incentives to create. Apple's claims that CORSEC competes with *other* Apple software is irrelevant. If those products compete with CORSEC, it is only because they, like CORSEC, make transformative use of iOS. And "copyright owners may not preempt exploitation of transformative markets." *Castle Rock Ent., Inc. v. Carol Publ'g Grp., Inc.*, 150 F.3d 132, 145 n.11 (2d Cir. 1998).

Finally, even if there were some cognizable financial harm to Apple (which there is not), it would be more than offset by the public benefit of Corellium's use. CORSEC advances the central copyright values of research and expansion of knowledge, while promoting informed public debate over important questions about the nation's cybersecurity and Apple's stewardship of its ecosystem. Of course, like all knowledge, the insights gained through CORSEC can be used for good or ill. But that is no basis for denying fair use, particularly given the dearth of evidence that CORSEC has ever been used for illegal or improper purposes and the abundant evidence of its use for socially beneficial applications. Moreover, denying fair use based on Apple's complaints about

Corellium's vetting and monitoring of its customers would necessarily put courts in the position of using copyright law as a source for regulating the details of cybersecurity research, a role for which neither the Copyright Act nor the courts are well suited.

That Apple separately registered copyrights for some wallpapers and icons does not alter the result, particularly given the lack of any evidence that CORSEC's failure to excise these aspects of iOS from the IPSW files harms any market for Apple's copyrighted works.

II. Apple faults the district court for failing to separately analyze its contributory infringement claims, but that is only because Apple made no separate contributory infringement arguments in opposing Corellium's fair use defense. In addition to being forfeit, Apple's new appellate arguments are meritless. Corellium can be charged only with customer uses it *promotes*. And Corellium promotes only those uses the district court addressed in rejecting Apple's direct infringement claims. Apple's insinuation that Corellium encouraged the discovery and sale of exploits for unlawful purposes has no foundation in the evidence and is no basis for denying fair use.

ARGUMENT

Corellium's CORSEC software provides researchers a tool for closely inspecting Apple's iPhone operating system so they can understand how it works and what its bugs and vulnerabilities may be. CORSEC does not contain any Apple code. Instead, Corellium's customers use CORSEC in conjunction with iOS files that Apple makes available for free download on the internet, without any licensing restrictions on their use. One might wonder how helping users inspect and understand such freely distributed files could constitute infringement in the first place. But the district court did not reach that question because even accepting Apple's description of how its iOS software is acquired and used,[12] and even assuming those uses are

[12] Apple asserts, for example, that Corellium directly provides users copies of iOS, based on evidence of a single instance. *See* Br. 9. *But see supra* n.7. Apple further attributes every action taken by Corellium's software at the direction of an end user—or even actions directed by iOS itself, such as displaying wallpaper art—to Corellium, rather than its customers or iOS. *See* Br. 9, 34. Corellium denies that it, rather than its users, copies iOS, but since the district court found fair use regardless of whether infringement occurred, such distinctions make no difference to the outcome of this appeal.

infringing, Corellium was entitled to summary judgment under the Copyright Act's fair use exemption.

I. The District Court Properly Held That Corellium's Transformative Research Tool Makes Fair Use Of Apple's iOS Code.

"From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose." *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 575 (1994). Accordingly, Congress has declared that "the fair use of a copyrighted work, including such use . . . for purposes [of] . . . scholarship, or research, is not an infringement of copyright." 17 U.S.C. § 107. Applying the statute's four non-exhaustive factors, the district court rightly concluded that in this case, Corellium's research tool makes fair use of Apple's software.

A. The First Factor Favors Fair Use.

"The first factor in the fair-use analysis, the purpose and character of the allegedly infringing work, has several facets." *Suntrust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257, 1269 (11th Cir. 2001). These include "(1) the extent to which the use is a 'transformative' rather than merely superseding use of the original work and (2) whether the use is for a nonprofit educational purpose, as opposed to a commercial purpose." *Cambridge Univ. Press v. Patton*, 769 F.3d 1232, 1261 (11th Cir. 2014). The district court correctly found the first factor favors fair use. Doc. 783, pgs. 20-25.

1. Copying Computer Code To Study Its Functionality Is Transformative.

A work is "transformative" if it "adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message." *Campbell*, 510 U.S. at 579. "The central purpose of this investigation is to see, in Justice Story's words, whether the new work merely 'supersede[s] the objects' of the original creation," *ibid.* (citation omitted), by "serv[ing] the same 'overall function' as the original," *Patton*, 769 F.3d at 1262 (citation omitted).

Consistent with the statute's listing of "research" and "scholarship" as quintessential examples of fair use, 17 U.S.C. § 107, copying to "shed[] light on an earlier work" is an established transformative use. *Campbell*, 510 U.S. at 579; *see also Patton*, 769 F.3d at 1262. For example, in *Authors Guild v. Google, Inc.*, 804 F.3d 202 (2d Cir. 2015), the Second Circuit considered whether Google made fair use of millions of copyrighted books when it included them in a digitized database for its

Google Books project. Google allowed users to search the full text of every work in the database, identifying books that contained the user's search terms and displaying the search results with their surrounding context. *Id.* at 208-09. The Second Circuit found that Google's use was "highly transformative," *id.* at 216, because the purpose of the copying was to "make available significant information *about those books*" rather than simply superseding the original use by providing the full text of the book in digital form. *Id.* at 217; *see also, e.g.*, *A.V. v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009) (copying student assignments into database to facilitate detection of plagiarism transformative use because database served an "entirely different function and purpose than the original works"); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007) (same where defendant copied thumbnails of copyrighted images for internet search engine).

In the same vein, courts have regularly found that copying and manipulating computer code to understand its functional aspects is a transformative fair use. In *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000), for example, the defendants wanted to create a competitor to Sony's PlayStation video game console. To allow their system to run PlayStation games, they needed to replicate the PlayStation's basic input-output system (BIOS), a part of the console's operating system. *Id.* at 599. The defendants "reverse engineered" the Sony BIOS by observing its operation "in an emulated environment," *id.* at 600, just as Corellium's customers observe iOS's operation using CORSEC. *See id.* at 599. Sony sued, but the Ninth Circuit found fair use. It explained that while Sony's operating system "may be copyrighted as expression," it "also contains ideas and performs functions that are not entitled to copyright protection." *Id.* at 602. Those "unprotected ideas and functions of the code," the court continued, "are frequently undiscoverable in the absence of investigation and translation that may require copying the copyrighted material." *Ibid.* Copying that software "for the purpose of gaining access to the unprotected elements of Sony's software" was a transformative fair use. *Ibid.*

Other courts, including the Supreme Court and this Court, have reached the same conclusion. *See Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183, 1198-99 (2021) (citing *Connectix* with approval as example of "applying fair use to intermediate copying necessary to reverse engineer access to unprotected functional elements within a program"); *id.* at

1218-19 (Thomas, J., dissenting) (agreeing reverse engineering can be fair use); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1539 n.18 (11th Cir. 1996) ("[R]everse engineering may be a fair use" when necessary to "'gain access to the ideas and functional elements embodied in a copyrighted computer program[.]'") (citation omitted); *see also, e.g.*, *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 537 (6th Cir. 2004); *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 644-45 (7th Cir. 2003); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1513-14 (9th Cir. 1992); *Atari Games Corp. v. Nintendo of Am. Inc.*, 975 F.2d 832, 843-44 (Fed. Cir. 1992).

The Copyright Office agrees, finding that both reverse engineering generally, and security research in particular, are transformative fair uses. *See, e.g.*, U.S. Copyright Office, *Section 1201 of Title 17: A Report of the Register of Copyrights* 15 & n.88 (June 2017); U.S. Copyright Office, *Software-Enabled Consumer Products: A Report of the Register of Copyrights* 55 (Dec. 2016) (*Software-Enabled Consumer Products*); U.S. Copyright Office, *Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention* 300 (Oct. 2015) (*Sixth Triennial Review*).

2. *Corellium's Tool For Studying How iOS Functions Makes Transformative Use Of Apple's Computer Code.*

Corellium's tools for reverse engineering iOS are equally transformative. The purpose of iOS is to "make[] iPhone run," Apple Br. 5, allowing users to make telephone calls, send texts, surf the web, play games, and download and run other applications. *See* Doc. 783, pg. 3; Apple Br. 5-6; Doc. 472-2, pg. 6. CORSEC, in contrast, is a tool for "research" and "scholarship." 17 U.S.C. § 107. It is a "new product" that runs iOS in a "distinct and different computing environment," to reverse engineer iOS and understand *how* iOS performs its functions. *Google*, 141 S. Ct. at 1203. Far from simply allowing users to "'interact with [iOS]' as if the program were installed 'on an actual iPhone,'" Apple Br. 25 (citations omitted), CORSEC allows users to "see running processes, halt execution of the virtual device, amend the kernel, look at lists of files, clone snapshots, among other things—giving great introspection into aspects of iOS and its operation on iOS devices." Doc. 783, pg. 23. Apple admits that these are capabilities it "does not offer in connection with retail versions of iOS." Br. 10; *see also* Doc. 783, pg. 23.

At the same time, CORSEC omits much of the iOS functionality that is unnecessary to its transformative purpose but essential to iOS's intended use of running a consumer smartphone, such as the ability to make phone calls, send texts, or download apps from the App Store. *See supra* at 12.

None of this is disputed. And all of it makes nonsense of Apple's claim that CORSEC "just takes 'real iOS' and puts it on non-Apple hardware." Br. 22 (internal citations omitted). If that were all Corellium had done, no one would buy its product. Apple cannot seriously suggest that anyone would pay "thousands—even hundreds of thousands—of dollars," Br. 12, for the chance to swap out their iPhone for a bulky computer that is incapable of performing nearly anything users buy iPhones to do.[13]

Apple nonetheless insists that CORSEC simply ports iOS to "a different medium" and that any additional features and value it adds "makes no difference under the law." Br. 23, 25. Not so. One could just as easily describe Google Books as simply copying traditional books to a

[13] Apple says future versions of CORSEC may replicate some presently excluded features. Br. 42. But if that happened, it would be to allow researchers to understand how those features work and the potential vulnerabilities they create, not to turn CORSEC into an expensive substitute for iOS or iPhones.

new digital medium and adding a search feature. Yet that was enough in *Authors Guild* because providing "significant information" about the books Google digitized serves a different purpose than the original works. 804 F.3d at 217; *see also iParadigms*, 562 F.3d at 639 (allowing users to compare text of student papers to prior works in database is a transformative use). CORSEC serves the same transformative purpose by providing researchers information *about* how iOS works and what its flaws may be, something iOS on its own is not intended or designed to do.

Apple attempts to distinguish *Authors Guild* on the ground that Google "did not reveal so much text as to make it a potential substitute for the original books." Br. 32 (cleaned up). But as discussed in greater detail below with respect to factors three and four, while CORSEC's transformative purposes necessarily require researchers to analyze more of a copyrighted work than Google Books did, there is no evidence that doing so creates a potential substitute for iOS. *See infra* § I.D.

Moreover, a software tool can be transformative even when it exposes much of a work's copyrighted expression. *See, e.g.*, *Patton*, 769 F.3d at 1262 ("Even verbatim copying 'may be transformative so long as the copy serves a different function than the original work.'") (citation omitted); *see also Katz v. Chevaldina*, 2014 WL 2815496, at *6 (S.D. Fla. June 17, 2014) ("Even making an exact copy of a protected work may be transformative, provided the copy serves a different function than the original work.") (citation omitted).

Reverse engineering is a classic example. *See supra* at 23-25. Apple attempts to distinguish the reverse engineering cases as involving *intermediate* use of a copyrighted work to produce an end product with entirely original code. Br. 43. But reverse engineering is transformative not because it is an intermediate step in a larger process, but because it allows "access to unprotected functional elements within a program," *Google*, 141 S. Ct. at 1198, advancing research and knowledge, which are transformative ends in their own right. That is why, for example, it was fair use for the defendants in *Connectix* to use an emulator to study Sony's BIOS. 203 F.3d at 602-03 (copying protected when it is "'necessary' to gain access to the functional elements of the software itself") (citation omitted). Of course, a separate fair use question would have arisen if the defendants had copied parts of the BIOS *again* in their final product in a way that superseded the original use. *See id.* at 605-06. For *that* reason, it is relevant whether the end product of reverse engineering contains copyrighted code. But in this case, CORSEC is not the end product of reverse engineering; it is a *tool* used for reverse engineering. It uses iOS in the same way the emulator in *Connectix* used Sony's BIOS—to access the functional elements of Apple's software, not to supersede it.[14]

In any event, as *Google v. Oracle* illustrates, a use can be transformative even when a defendant includes copied code in its end product, so long as the new use does not merely supersede the original's. *See* 141 S. Ct. at 1202-03. Apple insists that unlike Google, "Corellium has not created a new and independent program." Br. 26. But CORSEC is obviously a new creative work. *See* Doc. 783, pgs. 12-13. Users pay for the value of the original tools CORSEC provides, not to obtain a copy of

[14] *Connectix* involved *two* versions of the emulator—the one used to reverse engineer Sony's BIOS and the final product, the Virtual Game Station, which allowed PlayStation games to be played on desktop computers. *See* 203 F.3d at 601. As Apple points out, the Ninth Circuit found the Virtual Game Station only "modestly transformative" because it served largely similar ends to Sony's copyrighted works (*i.e.*, playing video games). *Id*. at 606. But the Ninth Circuit did not question that the emulator used for reverse engineering—which is the analog of CORSEC in this case—was highly transformative given that it did *not* serve the same purpose as a PlayStation console. And even if CORSEC were analogous only to the Virtual Game Station, the Ninth Circuit still found that use transformative and fair. *Ibid*.

iOS (which they can download for free from Apple). In this respect, Corellium's product is no different than Google Books, which combined Google's independent software with copyrighted works of others to shed light on the nature of those prior works.

Apple is thus left to claim that "[s]ecurity research . . . is one of the purposes already served by" ordinary iPhones running iOS. Br. 27 (cleaned up). That is like saying Google Books was not transformative because scholars could manually search books for keywords by going to the library. It is not simply that CORSEC serves the same function more efficiently—although that would be transformative enough. *See Fox News Network, LLC v. TVEyes, Inc.*, 883 F.3d 169, 177 (2d Cir. 2018) (recognizing the "transformative purpose of enhancing efficiency"); *Connectix*, 203 F.3d at 605 (same). Instead, CORSEC makes possible numerous uses—*e.g.*, viewing system calls in real time "to deeply inspect" iOS—that are impossible using iOS alone. Apple Br. 27, 33.

Apple counters that prior to CORSEC, security research was historically "done on a stock iPhone running stock iOS." Br. 27 (quoting Doc. 817-1, pg. 96). Research about books was historically done by reading physical manuscripts, but that did not make such research one of the purposes already served by those books, nor did it make Google Books an unfair use. In any event, the cited testimony made clear that [redacted]. *See* Doc. 817-1, pgs. 94-95. Moreover, Apple's witness was explaining [redacted]. *See* Doc. 817-1, pgs. 94-95.

Apple's felt-need to develop tools that, it says, perform similar functions to CORSEC further disproves Apple's claims that "security research is 'one of the purposes'" of iOS. Br. 27. So does Apple's insistence that CORSEC cannot be safely deployed without extensive vetting and constraints on its use, Br. 51-52, when Apple will sell an iPhone to anyone and makes iOS available for download on the internet, no questions asked.

Apple notes that CORSEC can be used for things other than security research. Br. 28-29 (citing example of testing third-party applications). But Apple does not deny that security research is CORSEC's principal use. And it offers no evidence that *any* of CORSEC's other potential uses supersede iOS's original function. More importantly, the question is whether CORSEC itself makes transformative use of iOS, not what CORSEC users do with that knowledge. And in all its applications CORSEC serves the core transformative purpose of "shedding light on [the copyrighted] work." *Campbell*, 510 U.S. at 579.

Of course, all knowledge can be used for good or ill. Apple singles out the ability to use the knowledge gained from CORSEC to develop and sell exploits. Br. 28-29. We address these arguments in detail when discussing factor four. But for present purposes, it suffices to observe that Apple's complaints about CORSEC's utility in helping uncover vulnerabilities only confirms that the product serves a transformative purpose distinct from iOS's.

3. The Commercial Nature Of Corellium's Product Does Not Shift The First Factor In Apple's Favor.

The district court also correctly determined that the commercial nature of CORSEC "does not undermine its fair use." Doc. 783, pg. 25. Because the "goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works," the "more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use." *Campbell*, 510 U.S. at 579. Here, CORSEC's use is highly transformative and poses no commercial threat to iOS. *See infra* § I.D. Withholding fair use protection simply because Corellium charges for its product would predictably reduce the availability of such transformative software tools, given the intensive investment of resources necessary to create them.[15]

B. The Second Factor Favors Fair Use.

The second factor examines the "nature of the copyrighted work." 17 U.S.C. § 107(2). In this case, the factor favors fair use because security research focuses on the functional aspects of computer code that fall outside the core of copyright protection. Moreover, copyrights in

[15] Apple accuses the district court of finding that the commercial nature of Corellium's use affirmatively favored a finding of fair use. *See* Br. 35. But its only support for that assertion is the final sentence of the section of the opinion addressing the first factor, where the court briefly summarized its prior discussion. *See ibid*. (quoting Doc. 783, pgs. 25-26 ("Therefore, both facets of the first factor favor a finding of fair use.")). In context, the court was simply referring to its earlier conclusion that "Corellium's profit motivation does not *undermine* its fair use defense, particularly considering the public benefit of the product" and its transformative nature. Doc. 783, pg. 25 (emphasis added).

operating systems, like iOS, give rise to a heightened risk of abuse by companies intent on extending their copyright monopoly to other markets, as illustrated in this case.

1. Apple's Predominantly Functional Computer Code Falls Outside The Core Of Intended Copyright Protection.

The second factor "calls for recognition that some works are closer to the core of intended copyright protection than others, with the consequence that fair use is more difficult to establish when the former works are copied." *Campbell*, 510 U.S. at 586. "Thus, copyright's protection may be stronger where . . . it serves an artistic rather than a utilitarian function." *Google*, 141 S. Ct. at 1197.

Although it has creative aspects to it, computer code is largely utilitarian. *See Google*, 141 S. Ct. at 1198. Apple points out that there are some forms of computer code that are less creative than others. Br. 36-37. But even the most creative code is still predominantly functional and utilitarian. 141 S. Ct. at 1198. And as the Copyright Office has explained, "works that are functional—like software embedded in and critical to the functioning of a consumer product—are entitled to lesser protection under the Copyright Act." *Software-Enabled Consumer Products*, *supra* at 58; *see also Connectix*, 203 F.3d at 603 (software "lies at a distance from the core" of copyright); *Sega*, 977 F.2d at 1526 (works that contain unprotected functional elements are accorded a "lower degree of protection than more traditional literary works").

Moreover, copyright protects only the creative *expression* embodied in how a program is written; it does not provide the author a monopoly in how the software functions. *See Mnemonics*, 79 F.3d at 1547 n.33 (warning that copyright protection must not "be extended to functional results obtained when program instructions are executed"). Accordingly, the public is free to examine and even copy software's ideas and functions. *See ibid.*; *Connectix*, 203 F.3d at 605. However, unlike other works, the "unprotected ideas and functions of [software] code" are "frequently undiscoverable in the absence of investigation and translation that may require copying the copyrighted material." *Connectix*, 203 F.3d at 602; *see also Software-Enabled Consumer Products*, *supra* at 42 (same). Allowing software developers—alone among copyright holders—to prevent the public from accessing the unprotected aspects of their works runs counter to the purpose of copyright to promote the progress of science and the useful arts, and to the Copyright Act's premise that "copyrights protect 'expression' but not the 'ideas' that lie behind it."

Google, 141 S. Ct. at 1196; U.S. Const. art. I, § 8, cl. 8; 17 U.S.C. § 102(b). It also risks affording software companies patent-like monopolies in their software's functionality without requiring them to meet the far more rigorous requirements for obtaining a patent. *See Connectix*, 203 F.3d at 605.

In this case another feature of iOS is also relevant: Apple allows the public to download it for free without any licensing restrictions. Doc. 783, pg. 5. That fact makes clear that Apple is not seeking to protect its copyrighted *expression* (which anyone can view by simply downloading IPSW files), but rather is seeking to leverage its copyright to preclude Corellium from making iOS's unprotected functionality available for close inspection.

2. *The Potential For Abuse Of Copyrights In Operating Systems Weighs In Favor Of Fair Use.*

The risk of extending the copyright monopoly beyond what Congress intended is particularly significant in cases, such as this, involving a computer operating system.

The Ninth Circuit's decision in *Sega* provides an apt illustration. There, as in the *Connectix* case discussed earlier, a maker of video game consoles owned a copyright in the console's operating system. That copyright, however, did not entitle Sega to exclude others from writing their own original gaming software for the consoles. Sega nonetheless attempted to extend its monopoly to compatible games by programming its operating system to play game cartridges only if they included a secret authorization code. 977 F.2d at 1515. Another company that wanted to produce games for the system made a copy of Sega's operating system in order to reverse engineer the authorization code. *Id*. at 1514-15. The Ninth Circuit held the copying to be fair use. Among other things, it explained that "an attempt to monopolize the market by making it impossible for others to compete runs counter to the statutory purpose of promoting creative expression and cannot constitute a strong equitable basis for resisting the invocation of the fair use doctrine." *Id.* at 1523-24.

Other courts, confronting similar attempts to extend the copyright monopoly, have likewise applied fair use to prevent such overreach. *See, e.g.*, *Lexmark*, 387 F.3d at 545 (printer manufacturer attempted to monopolize market for compatible toner cartridges by requiring cartridges to include software lock code discoverable only through copying and inspection of copyrighted software); *Connectix*, 203 F.3d at 607 ("Sony understandably seeks control over the market for devices that play games Sony produces or licenses. The copyright law, however, does not confer such a monopoly."). In *Google*, the Supreme Court cited these cases approvingly as illustrations of fair use ensuring that copyrights do not impose "unrelated or illegitimate harms in other markets or to the development of other products." *Google*, 141 S. Ct. at 1198.

In this case, Apple uses its copyright in iOS to extend its monopoly to other spheres. For example, Apple has designed iOS to preclude users from installing software from any source other than Apple's proprietary App Store, where it charges an extraordinary 30% commission on the creative work of thousands of third-party developers. *See supra* at 5. Consumers can avoid that monopoly only by jailbreaking their iPhones using exploits discovered through security research. *See supra* at 7. But as explained, security research inevitably requires copying and modifying iOS, whether through using a product like CORSEC or a rack of jailbroken iPhones. Accepting Apple's claims that such tools are derivative works of iOS, and that such use and modification of its software is not fair use, *see* Br. 46-48, would give Apple significant power to control the market for security research tools *and* protect its App Store monopoly, *see* Br. 8, 48, 51 (asserting the right to limit researchers to

Apple's proprietary research tools and to require them to report exploits to Apple so it can patch them before they become public, thereby preventing jailbreaks).

Thus, accepting Apple's arguments would ultimately give the company broad powers to dictate how and when many researchers can publicize their findings, and therefore significant control over knowledge and timely public discourse about its products—the exact opposite of what copyright law is intended to do.

C. The Third Factor Favors Fair Use.

The third factor asks "whether defendants have 'helped themselves overmuch' to the copyrighted work in light of the purpose and character of the use." *Peter Letterese & Assoc. v. World Inst. of Scientology Enters., Int'l*, 533 F.3d 1287, 1314 (11th Cir. 2008) (quoting *Campbell*, 510 U.S. at 587). In particular, the "inquiry is whether the amount taken is reasonable in light of the purpose of the use and the likelihood of market substitution." *Id*. at 1314 n.30. The district court rightly found that this factor, too, favors fair use. Doc. 783, pgs. 27-30.

1. *Copying The Entirety Of A Work Is Consistent With Fair Use When Necessary For A Transformative Purpose.*

As Apple admits, the third factor does not simply ask whether the defendant copied a little or a lot. Instead, the question is whether the amount of copying was "'necessary' to achieve a transformative purpose." Apple Br. 38 (quoting *Authors Guild*, 804 F.3d at 221); *see also Google*, 141 S. Ct. at 1205 (third factor "will generally weigh in favor of fair use where, as here, the amount of copying was tethered to a valid, and transformative, purpose"). Sometimes, a transformative purpose requires copying an entire work. *See, e.g.*, *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 449-50 (1984) (copying entirety of television show fair use); *Authors Guild*, 804 F.3d at 221 (entirety of millions of books); *Katz v. Google Inc.*, 802 F.3d 1178, 1183-84 (11th Cir. 2015) (per curiam) (entire photo); *iParadigms*, 562 F.3d at 642 (entirety of student papers).

2. *The Amount Of Copying Is Necessary To CORSEC's Transformative Purpose.*

The Copyright Office has explained that "it is often necessary to copy significant portions of the code to engage in reverse engineering activities." *Software-Enabled Consumer Products*, *supra* at 58. This case is no exception. Apple does not seriously dispute that researchers must copy iOS to research its functions and flaws. Doc. 783, pg. 29. Apple argues instead that it was not necessary to emulate "the entirety of iOS to accomplish" that transformative purpose. Br. 40-41. That claim has no merit.

Security research necessarily examines how the overall operating system functions in response to a variety of inputs and in conjunction with a wide range of third-party applications. To properly test and understand how an actual iPhone would perform in the hands of actual end users, a researcher must interact with broad swaths of the operating system, including its graphical user interface, icons, and wallpaper, as would a regular user. After all, vulnerabilities can, and do, arise in unexpected places. *See, e.g.*, Charlie Osborn, *LokiBot Malware Now Hides Its Source Code in Image Files*, ZDNet (Aug. 7, 2019).[16]

If Apple is suggesting that Corellium should provide different versions of CORSEC tailored to each user's specific interests, Apple cites

[16] https://www.zdnet.com/article/lokibot-information-stealer-now-hides-malware-in-image-files/.

no evidence or authority to support it. *See* Br. 41; *see also, e.g.*, *Connectix*, 203 F.3d at 605 (fair use does not require researchers to "follow the *least efficient solution*" or engage in "'wasted effort[s]'" simply to avoid infringement liability) (citation omitted). Even if it were technically and economically feasible to create individualized versions of CORSEC, it is impossible for researchers to know in advance what aspects of the complex interrelated software system will require examination or where that research will lead. In this respect, CORSEC is similar to Google Books, which copied millions of books to ensure it could serve unpredictable needs of all its users. *Authors Guild*, 804 F.3d at 208.

Apple insists that *Authors Guild* is distinguishable because Google displayed only a small portion of any work turned up in a search. *See* Br. 41. This argument fails for multiple reasons. First, Apple elides the distinction between revealing iOS's copyrighted expression and reproducing its unprotected functionality. When CORSEC produces a facsimile of an iPhone on a computer screen, illustrating how it would appear when running certain software on certain hardware with particular inputs, it reproduces iOS's functionality without revealing *any* of Apple's copyright code. Likewise, CORSEC's console displays a real-time textual *report* of system calls, not the underlying code that makes them. Doc. 472-32, pg. 58.

Second, when CORSEC does reveal parts of Apple's code, it is because that portion of code is of interest to a particular researcher, in the same way that Google Books reveals only the text that is responsive to a researchers' search terms. The fact that CORSEC opens the entirety of the work to such *potential* examination does not distinguish this case from *Authors Guild*, where "every nook and cranny" of each copyrighted work was subject to search. Apple Br. 43.

To be sure, the nature of security research may require users to view more than mere "snippets" of iOS's code. But Apple itself makes iOS (including icon and wallpaper files) available for unfettered public download, copying, inspection, and display. Moreover, *Authors Guild* explained that the critical inquiry is whether the product reveals more of the copyrighted work than is necessary for the transformative purpose and, in particular, whether the copyrighted expression is revealed "in such a manner" that it offers "a competing substitute for the original." 804 F.3d at 221; *see also Letterese*, 533 F.3d at 1314 ("Like the preceding factors, this factor is intertwined with the fourth factor and partly functions as a heuristic to determine the impact on the market for the original."). And as discussed next, there is no evidence that researchers' ability to view Apple's code renders CORSEC a market substitute for iOS.

D. The Fourth Factor Favors Fair Use.

The fourth and "undoubtedly the single most important element of fair use" is "'the effect of the use upon the potential market for or value of the copyrighted work.'" *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 566 (1985) (quoting 17 U.S.C. § 107(4)). The "more transformative the secondary use, the less likelihood that the secondary use substitutes for the original." *Letterese*, 533 F.3d at 1310 n.25; *see also Campbell*, 510 U.S. at 591. Moreover, given that the goal of fair use is to balance the social costs of copyright against the need to provide an incentive to create, it is not enough simply to show *some* harm from substitution. The fourth factor weighs against fair use only if the harm is "substantial." *Campbell*, 510 U.S. at 593 & n.23; *see also, e.g.*, *Connectix*, 203 F.3d at 607. And even then, the amount of the harm must be weighed against the "public benefits the copying will likely produce." *Google*, 141 S. Ct. at 1206.

1. *Corellium's Research Tool Does Not Materially Damage The Market For iOS Or Diminish Apple's Incentives To Create.*

The district court correctly found that "there is no evidence that the Corellium Product has affected, let alone materially affected, Apple's market or the market value for iOS." Doc. 783, pg. 30. To start, Apple cannot explain how CORSEC damages a market for iOS itself. The Copyright Office has explained that "[s]ecurity research is not likely to interfere with any market that the copyright owner is likely to exploit, because there is no market for the programs themselves, and they have no value apart from the device they operate." *Software-Enabled Consumer Products*, *supra* at 51. So too here. Apple does not sell iOS separate from Apple hardware; it gives the software away for free on the internet.

Apple nonetheless claims that CORSEC harms the market for *other* Apple products, including certain existing and future software tools as well as the market for physical iPhones. Br. 46-48. Even if those arguments could be countenanced under the fair use inquiry, which focuses on the potential market for the allegedly infringed work itself, those arguments lack merit.

Apple's Other Software. Apple points to certain software products—specifically "iOS Simulator" and an allegedly forthcoming product called "Xcode Cloud"—that it says compete with CORSEC. Br. 47-48. Even if Apple's development tools provided the same kind of functionality as CORSEC,[17] it would make no difference.

Copyright protects Apple from competition in the market for genuine derivatives of iOS, but not from competition in markets for transformative uses. *See Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 614-15 (2d Cir. 2006) (harm must be "to a traditional, as opposed to a transformative market"); *Castle Rock Ent., Inc. v. Carol Publ'g Grp., Inc.*, 150 F.3d 132, 145 n.11 (2d Cir. 1998) ("[C]opyright owners may not preempt exploitation of transformative markets[.]"). Thus, in *Authors Guild*, the court rejected publishers' claim that Google Books competed with search tools they could create as derivative works of the books they published. The court explained that true derivative works "generally involve . . . *changes of form*," such as turning a book into

[17] *But see* Doc. 783, pgs. 30-31 (rejecting Apple's reliance on marketing materials to prove similarity of products and actual market effects).

a movie. 804 F.3d at 215-16. In "contrast, copying from an original for the purpose of . . . provision of information *about* it" constitutes a transformative use. *Ibid*. (emphasis added). "Nothing in the statutory definition of a derivative work, or of the logic that underlies it, suggests that the author of an original work enjoys an exclusive derivative right to supply information about that work of the sort communicated by Google's search functions." *Id*. at 216. The same is true here. If Apple makes other products that serve the same transformative purpose as CORSEC, that simply means that Apple has elected to compete with Corellium in a different market, one in which Apple holds no lawful monopoly. Doc. 783, pg. 31.

At all events, there is no evidence that any potential harm to the markets for iOS Simulator or XCode Cloud is sufficiently "substantial" to tip the fourth factor in Apple's favor. *Campbell*, 510 U.S. at 593. The ultimate question is whether CORSEC captures so much of the market for iOS and its genuine derivatives that the "value of the remaining market is so diminished that it no longer makes economic sense for the author—or a subsequent holder of the copyright—to propagate the work in the first place." *Patton*, 769 F.3d at 1258. Here, Apple points to no evidence that anyone has ever forgone purchasing iOS or its derivatives, or even any of Apple's allegedly competing products, in favor of licensing CORSEC instead. Nor is there reason to think they ever would, given that Apple offers its products without additional cost to every developer who pays a $99 annual fee for access to a broad suite of development tools. Doc. 518-4, pg. 11. And even if every security researcher in the country forewent that $99 subscription in favor of a multi-thousand-dollar CORSEC license, Apple cannot plausibly claim that the minuscule loss in revenue would materially diminish its incentive to create and invest in iOS, which drives Apple's sale of billions of devices. *See* Doc. 1, pg. 6.

Physical iPhones. Apple's reliance on CORSEC's alleged effect on the sale of physical iPhones (Br. 46-47) fails as well.

To start, the fourth factor considers the effect on the "market for or value of the *copyrighted work*." 17 U.S.C. § 107(4) (emphasis added). And as Apple itself insists, "the copyrighted work at issue is iOS, not iPhone devices," meaning that only harm to "Apple's 'actual or potential markets for [iOS]' matters." Br. 50 (quoting *Google*, 141 S. Ct. at 1206) (alteration by Apple). Apple does not, and cannot, claim that iPhones are derivative works. *See* 17 U.S.C. § 101. Accordingly, any alleged injury to Apple's iPhone sales is irrelevant as a matter of law. Doc. 783, pg. 31; *see, e.g.*, *Lexmark*, 387 F.3d at 545 (rejecting printer company's reliance on reduced sales of printer cartridges due to competitor's reverse engineering its printer software); *Sony Computer Ent. Am., Inc. v. Bleem, LLC*, 214 F.3d 1022, 1029 (9th Cir. 2000) (refusing to consider collateral effects on video game sales where defendant copied screen shots of games).

In any event, Apple cannot plausibly claim that its authorship incentives are materially affected by CORSEC's potential effect on iPhone sales. As discussed, CORSEC is a wholly unsatisfactory substitute for ordinary iPhone users. *See supra* at 12. Apple is therefore forced to hypothesize that CORSEC is eating into its sales of "racks of physical devices" that otherwise would be bought for security research. Br. 47 (citation omitted). But, again, even giving Apple the benefit of every doubt, there is no reason to believe that there are enough researchers buying enough iPhones to meaningfully affect Apple's revenues or incentives even if (counterfactually) every single one of them purchased a CORSEC license instead.

The same is true of the even smaller number of specialized iPhones Apple may provide at no additional cost to certain subscribers to its Developer Program. Apple Br. 46. And even if, [redacted] its Security Research Device offered functionality akin to CORSEC's, it would only be because both tools put iOS to a transformative use.

2. *Any Effect On Apple's Incentive To Invest In iOS Is Far Outweighed By The Public Benefit Of Corellium's Tool.*

Even if there were reasons to think that CORSEC somehow harmed the iOS market, any reduction in Apple's incentive to create would be counterbalanced by "the public benefits the copying will likely produce." *Google*, 141 S. Ct. at 1206.

a. CORSEC directly advances "copyright's concern for the creative production of new expression," 141 S. Ct. at 1206, and "promot[ing] the Progress of Science and useful Arts," U.S. Const. art. I, § 8, cl. 8. It is a powerful research tool for understanding the operation of one of the nation's most critical pieces of software. The results of that research can promote and inform important public debates, including over whether Apple is adequately protecting users' security and privacy or the need for government regulation. *See Sixth Triennial Review*, *supra* at 300 (noting security "research activities may result in criticism or comment about the work").

In addition, CORSEC "allows creative new computer code to more easily enter the market." *Google*, 141 S. Ct. at 1208. For one thing, CORSEC can be used for testing by third-party developers on the myriad combinations of devices and operating system versions that exist in the market, facilitating the creation of new apps. *See* Apple Br. 29, 47. Third-party security research also fosters public and developer confidence in the platform, thereby encouraging developer investment in the ecosystem.

Apple recently acknowledged third-party researchers' role in bolstering public confidence in its platform when it faced privacy objections over its plans to inspect users' photo albums for evidence of child pornography. Apple sought to reassure consumers that it would not subsequently broaden the scope of its review, explaining that independent researchers could "verif[y]" Apple's claims because they are "constantly able to introspect what's happening in Apple's [phone] software." Patrick Howell O'Neill, *Apple Says Researchers Can Vet Its*

Child Safety Features. But It's Suing a Startup That Does Just That, MIT Tech. Rev. (Aug. 17, 2021) (alteration in original).[18]

b. Apple does not deny that CORSEC provides these benefits. Instead, it focuses exclusively on the prospect that CORSEC users will use the knowledge they gain to create "exploits," some of which could be used by cybercriminals. Br. 51-52. As discussed below, Apple offers no genuine evidence of CORSEC being used for illegal purposes, relying instead on speculation and innuendo. But the argument fails at the outset for an even more fundamental reason.

While fair use analysis takes into account a work's ability to serve copyright's purposes by promoting research, the advancement of knowledge, and the creation of new works, the Supreme Court has been clear that courts are ill suited to pass judgment on what the public does with the knowledge gained or on the creativity an otherwise fair use unleashes. In *Campbell*, for instance, the Court quoted Justice Holmes's admonition that "it would be a dangerous undertaking for persons

[18] https://www.technologyreview.com/2021/08/17/1032113/apple-says-researchers-can-vet-its-child-safety-features-its-suing-a-startup-that-does-just-that/.

trained only to the law to constitute themselves final judges of the worth of a work, outside of the narrowest and most obvious limits." 510 U.S. at 582 (quoting *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 251 (1903)) (brackets omitted). It is just as dangerous for judges to pass judgment on the otherwise lawful uses to which the public puts the knowledge gained by transformative research tools. In *Authors Guild*, for example, the Second Circuit did not ask how researchers might use the knowledge they acquired using Google Books.

This case illustrates the wisdom of that restraint. Apple would have this Court declare, as a matter of copyright law, that the discovery and sale of exploits is contrary to the public interest. Br. 51. Indeed, Apple implies that even public disclosure of security flaws conflicts with the public interest. *See ibid.* (security research "serves the public interest only when limited to identifying vulnerabilities that are reported back to" Apple). The Copyright Office disagrees. *See Software-Enabled Consumer Products*, *supra* at 44 ("There are significant benefits to allowing security researchers to study software-enabled consumer products for potential vulnerabilities and to *share their findings with the general public.*") (emphasis added). Presumably so would the law enforcement and national security agencies that rely on such exploits for their important public missions.

Apple points to nothing in the text of the Copyright Act or the traditions of copyright law that could help this Court decide who is right, much less to dictate the manner of customer vetting and monitoring required for lawful sale of security research tools. *See* Br. 51-52. Indeed, judges and jurors are far less equipped to set the rules for cybersecurity research than they are to say whether a parody is good or bad. *See Campbell*, 510 U.S. at 582; *cf. Connectix*, 203 F.3d at 605 (declining to "supervise the engineering solutions of software companies in minute detail" in the name of fair use); *Software-Enabled Consumer Products*, *supra* at 44 (reaffirming Copyright Offices' position that "rules governing security research 'hardly seem the province of copyright, since the considerations of how safely to encourage such investigation are fairly far afield from copyright's core purpose of promoting the creation and dissemination of creative works.'") (quoting *Sixth Triennial Review*, *supra* at 316).

Nor is there a compelling need to press the fair use doctrine into service as a source of cybersecurity regulation. Engaging in or assisting cybercrimes is already subject to serious criminal punishment. *See, e.g.*, 18 U.S.C. §§ 2, 1030. And Congress previously amended the Copyright Act to address cybercrime in the DMCA, adding provisions Apple relied on in its complaint but ultimately dismissed. *See* 17 U.S.C. § 1201; Doc. 1013. If more is needed, "cybersecurity issues relating to software-enabled consumer products are being studied by other parts of the government," which can act with far greater insight and clarity than the courts or juries engaged in case-by-case fair use analysis. *Software-Enabled Consumer Products*, *supra* at 44 (citing Department of Commerce's Internet Policy Task Force).

c. All that said, if this Court were inclined to evaluate the uses to which Corellium's customers put the knowledge they gain using CORSEC, the summary judgment record confirms the overwhelmingly beneficial uses of the product and the lack of any genuine evidence of its misuse.

The third-party security research performed by CORSEC's users indisputably advances the public interest. As the President recently noted, the "United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." Exec. Order 14,028, § 1, 86 Fed. Reg. 26,633 (May 12, 2021).[19] And experience has shown that we cannot leave cybersecurity to platform developers like Apple—independent researchers routinely find security vulnerabilities that Apple has missed. *See, e.g.*, Gordon Kelly, *New iPhone iMessage Flaw Enables 'Zero Click' Hack*, Forbes (Aug. 25, 2021)[20]; Christopher Bing & Joseph Menn, *Flaw in iPhone, iPads May Have Allowed Hackers to Steal Data for Years*, Reuters (Apr. 22, 2020).[21]

Apple also does not dispute the social value of other uses it identifies, such as testing third-party apps. *See* Br. 29. Instead, Apple pins its entire argument on its unsupported claim that "Corellium actively encourages customers to sell vulnerabilities with 'real exploits'

[19] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[20] https://www.forbes.com/sites/gordonkelly/2021/08/25/apple-iphone-warning-pegasus-hack-upgrade-ios-14-security/?sh=125d43c3229d.

[21] https://www.reuters.com/article/us-usa-applecyber/flaw-in-iphone-ipads-may-have-allowed-hackers-to-steal-data-for-yearsidUSKCN2242IK.

to the highest bidder" and allegedly does not do enough to "guard against its product falling into the wrong hands." Br. 51. That argument has no merit.

Any technology may be used for good or ill. That is certainly true of iOS and the iPhone. Apple's security and other features make its devices attractive to criminals and terrorists around the world. Nonetheless, Apple does not vet or monitor its customers to prevent its products from used for harmful or illegal purposes. *See supra* at 6. [redacted]. Doc. 472-1, pg. 92. Moreover, despite its claim that security research "serves the public interest only when . . . vulnerabilities . . . are reported back to the company" that can fix them, Br. 51, "Apple does not impose that requirement under its own Bug Bounty Program," Doc. 783, pg. 32. And in at least one instance, a "security researcher in Apple's Security Bug

Bounty Program has had his bugs used by China against Uyghurs, an ethnic minority group primarily living in China." *Ibid*.

Given this, Apple's complaints about Corellium's vetting and monitoring practices are "puzzling, if not disingenuous." Doc. 783, pg. 32. They are also unfounded. As the district court explained, Corellium takes significant steps to prevent misuse of its product. *Ibid*. It engages in meaningful vetting of potential customers, has refused licenses to those it suspects will abuse the product, prohibits illicit uses of its product in the licensing agreement, and has terminated user access based on concerns that its product was being used for ill. *See supra* at 12-13.

But even if Apple's vetting and monitoring complaints had some basis, they would simply show, at most, the *possibility* that CORSEC could be used for harmful ends. But Apple never actually claims that CORSEC *has* been used for illegal purposes, although it tries mightily to imply otherwise. *See* Br. 51-52. For example, Apple states that Corellium's marketing materials encourage sales "to the highest bidder," implying that Corellium promotes indiscriminate sales without regard to the lawfulness of the intended use. Br. 51. But the cited materials do not use that term; they only claim that sales can be lucrative. *See ibid*.

(citing Doc. 470-21, pg. 2 ("We run real iOS – with real bugs that have real exploits."); Doc. 470-23, pg. Corellium-009105.000006 ("A single vulnerability discovered or maintained with Corellium could easily be worth more than the software itself.")). And as discussed, exploits can profitably by sold to Apple itself, as well as to others for lawful use in security research, law enforcement, and national security operations.[22]

In the end, this Court need not separate the sinners from the saints in this case. "[C]opyright is not a privilege reserved for the well-behaved," *Google*, 141 S. Ct. at 1204 (citation omitted), and neither is fair use, *see ibid.* (declining to decide whether an alleged infringer's bad faith "is as a general matter a helpful inquiry" where, as here, "the strength of the other factors pointing toward fair use" make it unnecessary); *Campbell*, 510 U.S. at 585 n.18.[23]

[22] Apple alleges that Corellium has sold to "borderline entities" in the past, as no doubt has Apple. But Apple does not assert that CORSEC was used for illicit purposes by these entities, much less that Corellium had reason to know the license would be used in harmful ways. Br. 52.

[23] When some courts considered a defendant's alleged bad faith prior to *Google*, they evaluated how the copying was conducted—*e.g.*, using a "purloined manuscript"—not how knowledge gained through a transformative work was used. *See, e.g.*, *NXIVM Corp. v. The Ross Inst.*,

E. The District Court Properly Entered Summary Judgment With Respect To Apple's Wallpaper And Icons.

Nothing about Apple's copyright in its wallpaper or icons requires a different result. Even assuming those items are protected and infringed,[24] Apple publicly distributes all those wallpaper and icon image files as part of its free IPSW downloads and presented no evidence that reproducing them affects the market for iOS, iPhones, or any other Apple product. Nor does Apple claim that there is an independent market for those works. *See Letterese*, 533 F.3d at 1317 (fourth factor takes into account effects "only [in] those markets that creators of original works would in general develop or license others to develop") (quoting *Campbell*, 510 U.S. at 592) (brackets omitted). The absence of market effect is fatal to these claims, particularly given the functional aspects of icons and

364 F.3d 471, 478 (2d Cir. 2004); *see also id*. at 479 n.2 (finding of such bad faith "is not to be weighed very heavily" and "cannot be made central to fair use analysis").

[24] *But see Apple Computer, Inc. v. Microsoft Corp.*, 799 F. Supp. 1006, 1034-36 (N.D. Cal. 1992) (finding Apple's functional icons and desktop representations not copyrightable under merger and *scénes á faire* doctrines), *aff'd*, 35 F.3d 1435 (9th Cir. 1994).

wallpaper files within the iOS graphical user interface and researchers' need to observe these features and functions in operation. *See supra* at 41-42; Doc. 783, pg. 29; *cf. NXIVM Corp. v. The Ross Inst.*, 364 F.3d 471, 480-81 (2d Cir. 2004) (rejecting proposition that authors can expand scope of copyright protection for broader work by obtaining separate registrations for subparts).

II. The District Court Properly Granted Summary Judgment On Apple's Contributory Infringement Claims.

Apple argues that even if Corellium's use of iOS is fair, Corellium's customers' uses may not be. Br. 53. Accordingly, Apple insists, it was error to dismiss its contributory infringement claims before Corellium established "what every single one of its customers . . . do[es] with the product" and proved that every such use is fair use. Br. 56. That argument is forfeit and meritless.

A. Apple Failed To Preserve Any Separate Fair Use Arguments Regarding Contributory Infringement.

Apple faults the district court for failing to separately analyze Corellium's fair use defense as applied to Apple's contributory infringement claims. Br. 53. But the court engaged in no separate analysis only because Apple made no separate argument. Although

Corellium moved for summary judgment against *all* of Apple's claims based on fair use, Doc. 813, pgs. 1, 20, Apple's opposition argued only that fair use was no defense to Corellium's own allegedly infringing uses. *See* Doc. 828-1, pgs. 11-19. Indeed, Apple insisted that "[t]he relevant use of iOS for purposes of the fair-use inquiry is Corellium's use, not its customers' uses." *Id.*, pg. 15. Thus, the fair use section of Apple's brief never mentioned contributory infringement or its inducement theory under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), a case it cited for the first time in this litigation in its opening brief to this Court. *Compare* Doc. 828-1, pgs. 11-19, *with* Apple Br. 53-58. This, even though Apple elsewhere insisted that its direct and indirect infringement claims required separate analysis for purposes of deciding whether Corellium was entitled to summary judgment on *infringement*. Doc. 828-1, pg. 8 n.3.

Apple should not be heard to complain that the district court failed to address arguments that Apple never made below. The argument is forfeit. *Bailey v. Metro Ambulance Servs., Inc.*, 992 F.3d 1265, 1273-74 (11th Cir. 2021) (per curiam).

B. Apple's Contributory Infringement Argument Fails.

Apple's argument is meritless in any event. Apple first asserts in passing that Corellium is liable under *Sony*'s "distribution" theory simply for selling CORSEC to end users. *See* Br. 57. That is incorrect. As Apple admits (*ibid.*), that form of liability does not apply if the product is "capable of substantial noninfringing uses." *Sony*, 464 U.S. at 442. And for the reasons already discussed, CORSEC meets that test.

Apple also argues, for the first time on appeal, that Corellium is liable under a separate *inducement* theory recognized in *Grokster*. Br. 57. Under that theory, Apple says, Corellium "may be held liable for contributory infringement if Corellium 'was aware of or encouraged' its customers to engage in 'infringing practices." Br. 53 (citation omitted). Apple then claims that Corellium encourages its customers to modify, clone, and share iOS using CORSEC. Br. 54. Corellium cannot defend those infringing uses on fair use grounds, Apple insists, because it cannot show that every such use was fair, given that "Corellium has no way of knowing" what its customers "are up to." Br. 56.

There are many things wrong with this argument. First, Apple misstates the standard for inducement-based infringement, which requires Apple to prove not simply that Corellium was "aware of" its customers' infringing practices, Br. 53, but that Corellium distributed its product "with the *object* of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement," *Grokster*, 545 U.S. at 936-37 (emphasis added); *see also id*. at 937 ("[M]ere knowledge of infringing potential or of actual infringing uses would not be enough").

Second, for this reason, Corellium need not prove that "every single one of its customers" puts CORSEC to fair use. Apple Br. 56. The only relevant customer conduct is that which Corellium "promot[ed]." *Grokster*, 545 U.S. at 936. Here, the only uses that Apple says Corellium promoted are those inherent in any use of Corellium's transformative product—copying, running, and modifying iOS in order to understand the software's unprotected functionality. Br. 54. Even setting aside the question of how Corellium's customers could be liable for these uses when Apple makes the software available for download without any licensing restrictions, those uses are fair use for the reasons already discussed. And without direct infringement by CORSEC users, there can be no contributory infringement by Corellium. *See, e.g.*, *Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 845-46 (11th Cir. 1990).

Apple suggests that the balance of fair use considerations might shift depending on the uses to which Corellium's customers put the knowledge they gain by using CORSEC. Br. 56-57. As discussed, that consideration is irrelevant to the fair use analysis. But even if it were not, the main uses—security research, reverse engineering, jailbreaking, developing exploits for law enforcement and national security agencies—redound overwhelmingly to the public benefit.

That then leaves Apple's insinuation that some customers may use exploits for nefarious purposes. Br. 57. But Apple points to no evidence that Corellium *promoted* that illegal use. Instead, the handful of statements it cites simply advertise CORSEC as useful for discovering exploits, which can then be sold. *See supra* at 59-60. Nothing in the cited material encourages sales to cybercriminals, as opposed to researchers, law enforcement, or Apple itself. And there is ample evidence that Corellium takes care to prevent its product from being put to illicit uses.

See supra 12-13.[25] On this record, no reasonable jury could find that Apple had proven "by clear expression or other affirmative steps taken to foster infringement" that Corellium was "promoting [CORSEC's] use to infringe copyright." *Grokster*, 545 U.S. at 936-37.

Accordingly, the district court had no reason to separately address the fair use defense's application to Apple's contributory infringement claims and did not err in entering final judgment in Corellium's favor on all counts.

[25] Apple's claim that Corellium supposedly licensed "borderline entities" is no basis for contributory infringement liability either. Even if, contrary to the evidence, Corellium *knew* that those entities would misuse CORSEC, "mere knowledge . . . of actual infringing uses would not be enough." *Grokster*, 545 U.S. at 937.

CONCLUSION

For the foregoing reasons, the district court's judgment should be affirmed.

February 10, 2022

Respectfully submitted,

/s/ Kevin K. Russell
Thomas C. Goldstein
Kevin K. Russell
GOLDSTEIN & RUSSELL, P.C.
7475 Wisconsin Avenue
Suite 850
Bethesda, MD 20814
(202) 362-0636

Seth D. Greenstein
CONSTANTINE CANNON LLP
1001 Pennsylvania Ave, NW
Suite 1300N
Washington, DC 20004
(202) 204-3514

Justin B. Levine
COLE, SCOTT & KISSANE, P.A.
Esperante Building
222 Lakeview Avenue, Suite 120
West Palm Beach, Florida 33401
(561) 612-3459

Counsel for Defendant-Appellee Corellium, Inc.

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume limit as set out in Fed. R. App. P. 32(a)(7), because it contains 12,865 words, excluding the parts of the document exempted by Fed. R. App. P. 32(f) and Circuit Rule 32-4.

2. This document 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 document has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in 14-point New Century Schoolbook LT Std font.

/s/ Kevin K. Russell
Kevin K. Russell

Counsel for Defendant-Appellee

CERTIFICATE OF SERVICE

I hereby certify that on February 10, 2022, I caused the redacted version of the foregoing brief to be electronically filed with the U.S. Court of Appeals for the Eleventh Circuit through the Court's CM/ECF system. Parties represented by registered CM/ECF users will be served by the CM/ECF system. By agreement, the sealed version of the foregoing was also served on counsel for all parties by email.

/s/ Kevin K. Russell
Kevin K. Russell

Counsel for Defendant-Appellee